العدد 22




# توقعات كبيرة:
# تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط

باتريك باولاك Patryk Pawlak
منسق
عادل عبد الصادق Adel Abdel-Sadek
صامويل دومينيوني Samuele Dominioni
ألكسندرا ماريون يمنى لبن Alexandra Marion Youmna Laban



العدد 22




# توقعات كبيرة:
# تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط

باتريك باولاك Patryk Pawlak
منسق

عادل عبد الصادق Adel Abdel-Sadek
صامويل دومينيوني Samuele Dominioni
ألكسندرا ماريون يمنى لبن Alexandra Marion Youmna





أصبحت **يورومِسكو (EuroMeSCo)** معياراً للبحوث والدراسات الموجِّهة للسياسات العامة حول القضايا المتعلقة بالتعاون الأورومتوسطي، ولا سيما تلك المتعلقة بالتنمية الاقتصادية والأمن والهجرة. ومن خلال 104 مراكز أبحاث ومؤسسة فكرية وحوالي 500 خبير من 29 دولة مختلفة، طورت الشبكة أدوات مؤثرة تعود بالفائدة على أعضائها وعلى طيف أكبر من المجتمع من ذوي المصلحة في المنطقة الأورومتوسطية.

فمن خلال مجموعة واسعة من المنشورات والدراسات الاستقصائية والفعاليات وأنشطة التدريب والمواد السمعية والبصرية وتواجد متزايد على وسائل التواصل الاجتماعي، تصل الشبكة كل عام إلى آلاف الخبراء والمفكرين والباحثين وصانعي السياسات والمجتمع المدني وأصحاب المصلحة في أوساط التجارة والأعمال. أثناء القيام بذلك، تشارك يورومِسكو بزخم في تنسيق وتأطير البحوث المشتركة الأصيلة التي يشارك فيها خبراء أوروبيون ومن جنوب المتوسط، كما تساهم في تشجيع التبادل بينهم بغية تعزيز التكامل الأورومتوسطي في نهاية المطاف. إن الرابط المشترك لجميع الأنشطة هو الالتزام العام بتعزيز مشاركة الشباب وضمان المساواة بين الجنسين ضمن مجتمع الخبراء الأورومتوسطي.

**يوروميسكو: ربط النقاط (EuroMesCo: Connecting the Dots)** هو عبارة عن مشروع بتمويل مشترك من قبل الاتحاد الأوروبي والمعهد الأوروبي للبحر الأبيض المتوسط ويتم تنفيذه في إطار شبكة يورومِسكو.

وكجزء من هذا المشروع، تجتمع كل سنة خمس فِرق دراسية مشتركة لإجراء بحوث قائمة على الأدلة وموجِّهة للسياسات. ويتم تحديد مواضيع البحوث للفِرق الدراسية الخمس من خلال عملية شاملة من المشاورات حول السياسات العامة هدفها تعيين المواضيع ذات الصلة. ويشارك في كل فريق دراسي منسقٌ وفريق من المؤلفين الباحثين الذين يعملون على إعداد بحوث حول السياسات العامة والتي تطبع وتنشر من خلال قنوات ومناسبات مختلفة، وتصاحبها مواد سمعية بصرية.

**دراسة السياسة العامة** POLICY STUDY

**الناشر:** المعهد الأوروبي للبحر الأبيض المتوسط
**مراجعة الاقران Peer Review**
مراجعة الأقران الأكاديمية: anonymous

**التحرير:** كارينا ملكونيان Karina Melkonian
**مصمم التنسيق:** Maurin.studio
**التصميم:** نوريا إسبارثا Núria Esparza
ردمك رقمي 2696–7626
تموز 2021

**تنسيق النسخة العربية**
Punt d´Intercanvi & Punt Comú
**الترجمة من الإنجليزية:** رجائي برهان
**تنضيد الحروف العربية:** أحمد الأحمد
**المراجعة اللغوية والتدقيق:** نزار فلّوح




**إن المعهد الأوروبي للبحر الأبيض المتوسط (IEMed)**، والذي تأسس عام 1989، هو مركز أبحاث وتنفيذ متخصص في العلاقات الأوروبية المتوسطية. ويقدم هذا المعهد بحوثاً موجهة للسياسات العامة وقائمة على الأدلة استناداً إلى تأطير أورومتوسطي شامل ومتعدد الأبعاد.

وفقاً لمبادئ الشراكة الأوروبية المتوسطية (EMP)، ولسياسة الجوار الأوروبية (ENP)، وللاتحاد من أجل المتوسط (UfM)، وفقاً وانسجاماً مع ذلك فإن هدف المعهد الأوروبي للبحر الأبيض المتوسط هو التحفيز على التفكير والعمل اللذين من شأنهما المساهمة في التفاهم المشترك، والتبادل والتعاون بين مختلف بلدان ومجتمعات وثقافات البحر الأبيض المتوسط، إضافة إلى تعزيز البناء التدريجي لفضاء من السلام والاستقرار والازدهار المشترك والحوار بين الثقافات والحضارات في حوض البحر الأبيض المتوسط.

إن المعهد الأوروبي للبحر المتوسط IEMed هو عبارة عن ائتلاف يضم الحكومة الكتلانية، وزارة الشؤون الخارجية والاتحاد الأوروبي والتعاون الإسبانية، والاتحاد الأوروبي، ومجلس مدينة برشلونة. كما يضم المجتمع المدني من خلال مجلس أمنائه ومجلسه الاستشاري.

# المحتوى:

# الموجز التنفيذي

إنّ تعاون الاتحاد الأوروبي (EU) في مجال الأمن السيبراني مع منطقة الشرق الأوسط وشمال أفريقيا (MENA) هو تعاون مشروط بمطلبين متعارضين. ونظراً للقرب الجغرافي والآثار الأمنية الواسعة على الاتحاد الأوروبي، تُعتَبَر منطقة الشرق الأوسط وشمال أفريقيا من أولويات العلاقات الخارجية للاتحاد الأوروبي؛ فعلى مدى العقدين الماضيين، وخاصّة بعد الربيع العربي، استثمر الاتحاد الأوروبي موارد كبيرة لدعم الإصلاحات في المنطقة، ومواءمة سياساته العامة مع سياساتها. غير أنّ هذا الطموح إلى التعاون الوثيق مع المنطقة كثيراً ما يزداد تعقيداً بسبب الحالة على أرض الواقع. وهذا هو الحال بالنسبة إلى التعاون في مجال المناعة السيبرانية بشكل خاصّ، فعلى الرغم من المصالح المتداخلة، مثل مكافحة الجريمة السيبرانية، أو تحسين المستوى العام للأمن السيبراني، يحتاج الاتحاد الأوروبي إلى ممارسة قدر كبير من الحيطة الواجبة من أجل تجنب تقويض حماية حقوق الإنسان الهشّة بالفعل في بعض تلك البلدان. ولا يزال التوفيق بين هذين العنصرين: الاستعداد للمشاركة في تعاون أوثق، والحاجة إلى نهج حذر للتعاون في مجال الأمن السيبراني، يشكل التحدي الرئيسي في هذا المجال.

وفي ظل هذه الخلفية، تهدف هذه الدراسة إلى الإجابة عن سؤالين، أولاً: إلى أيّ مدى تتوافق المبادرات والسياسات المختلفة المُنفَّذَة في جميع أنحاء المنطقة مع مصالح الاتحاد الأوروبي وقيمه؟ ثانياً: مَن هم اللاعبون الرئيسيون الذين يمكنهم أن يضاعفوا الأمن السيبراني في المنطقة، والذين يمكن أن يتماشوا مع الاتحاد الأوروبي في جوانب معينة، ويساعدوه على تحقيق أهدافه السياسية؟ أيٌّ من هذه العلاقات ناضجة بما فيه الكفاية أو تتطلب المزيد من العمل من أجل التحول إلى مبادرات تعاون ملموسة؟ توجِّه هاتان المجموعتان من الأسئلة المناقشة في كلّ فصل من الفصول التالية.

تتناول ألكسندرا ماريون يمنى لبن مسألة **الاقتصاد الرقمي والجريمة السيبرانية**. تشكل الهجمات السيبرانية، وسرقة الملكية الفكرية التي تسهلها الرقمنة، والاحتيال عبر الإنترنت، والتلاعب المالي تهديداً للاقتصاد الرقمي، وتتطلب استجابة سريعة من السلطات العامة. إنّ التحدي الذي تواجهه منطقة الشرق الأوسط وشمال أفريقيا لا يقتصر على إيجاد مكان لنفسها في هذا الاقتصاد العالمي الجديد، بل أيضاً في تحديث مؤسساتها العامة لمواجهة التهديدات الجديدة في الفضاء السيبراني. وبالإضافة إلى عرض الاتجاهات العامة، يدقّق الفصل الأول في مشاركة دول الشرق الأوسط وشمال أفريقيا في المناقشات الإقليمية والعالمية حول التعاون الدولي ضدّ الجريمة السيبرانية (مثل اتفاقية بودابست، الأمم المتحدة (UN)، المبادرات الإقليمية)، فضلاً عن تقديم توصيات حول تعاون الاتحاد الأوروبي مع منطقة الشرق الأوسط وشمال أفريقيا. ويتناول الفصل بصفة خاصة الحالة في الجزائر ولبنان والمغرب.

وينظر صامويل دومينيوني إلى تحدي المناعة السيبرانية نظرة أبعد من المنظور المجتمعي، ويحلّل الصلة بين **التحدي المزدوج للتحول الرقمي والتحول الديمقراطي** في جميع أنحاء المنطقة. ويتناول في الفصل الخاص به كيفية تأثير نموذج حوكمة الإنترنت على انتقال / تعزيز النظام في منطقة الشرق الأوسط وشمال أفريقيا. ويرى الفصل الثاني أنّ عدم وجود فهم مشترك ومبادئ مشتركة لإدارة الفضاء السيبراني يسمح للبلدان باعتماد سياسات مختلفة على الصعيد المحلي. ويحلّل الفصل على وجه الخصوص كيفية ومدى استخدام السياسات الرامية إلى الحدّ من المعلومات المُضَلِّلَة التي تُستخدَم لسحق المعارضة السياسية والحدّ من النفوذ الخارجي في الفضاء السيبراني. ويتناول الفصل الحلول المختلفة المعتمدة في الأردن والمغرب ومصر.

وأخيراً، ينظر باتريك باولاك إلى المسألة الأوسع نطاقاً المتمثلة في **منع نشوب الصراعات وتعزيز سلوك الدولة المسؤول في الفضاء السيبراني**. ويحلل الفصل الأخير كيفية تأثير المنافسة الجيوسياسية المتزايدة في الفضاء السيبراني على استقرار المنطقة. تستخدم دول مثل إسرائيل وإيران وتركيا بانتظام العمليات السيبرانية لدعم أهدافها السياسية. وبالإضافة إلى ذلك، فإنّ مشاركة القوات العسكرية للولايات المتحدة الأمريكية، واتساع وجود جهات فاعلة مثل الصين وروسيا في المنطقة يزيد من تعقيد الوضع. إنّ التطورات المتعلقة بالفضاء السيبراني في المنطقة توضح جيداً أنّ هذا الفضاء ليس سوى مجال إضافي لتحقيق الأهداف السياسية والاقتصادية، ولا سيّما في سياق صراع قائم من قبل. ومع ذلك، وباستثناء مصر وإيران، فإنّ غالبية دول المنطقة غائبة إلى حدّ ما عن المناقشات الدولية الرامية إلى تعزيز استقرار الفضاء السيبراني.

وبالتالي، فإنّ التحليل المقدم في هذه الدراسة يؤدي إلى أربع ملاحظات رئيسية:

- **التعارض بين مناعة الدولة والمناعة المجتمعية.** في حين أنّ بناء مناعة الدولة والمجتمع هو أحد أهداف الاتحاد الأوروبي، فإنّ هذين المفهومين غالباً ما يصطدمان في منطقة الشرق الأوسط وشمال أفريقيا: فالمجتمع القوي تعتبره بعض الحكومات تهديداً لحكمها وليس عنصراً تمكينيّاً. وحتى ينخرط الاتحاد الأوروبي في شراكة مجدية مع المنطقة بشأن السياسات السيبرانية والرقمية، يجب فهم هذا التوتر ومعالجته بشكل أفضل من خلال استراتيجيات ملائمة للتخفيف من المخاطر.

- **التعاون الدولي لمكافحة الجرائم السيبرانية**. الجريمة السيبرانية هي إحدى الأولويات الرئيسية للتعاون الدولي الذي تم تسليط الضوء عليه في *استراتيجية الاتحاد الأوروبي للأمن للفترة 2020-2025*. وبالإضافة إلى ذلك، فإن الجريمة السيبرانية هي أحد التهديدات التي تهدد الثقة في المجتمع والاقتصاد الرقميين اللذين يضعهما الاتحاد الأوروبي كأولوية من أولويات نموه. وثمّة شواغل مماثلة في منطقة الشرق الأوسط وشمال أفريقيا؛ ولذلك، فإنّ هناك أساساً متيناً للحوار بشأن تلك المسائل. بيد أنّ الافتقار إلى آليات مناسبة لحماية حقوق الإنسان والضوابط والموازين في بعض بلدان المنطقة لا يزال يشكل عائقاً خطيراً أمام توثيق التعاون.

- **الاستقرار والسلوك المسؤول في الفضاء السيبراني.** قام الاتحاد الأوروبي – من خلال نشاطاته في الأمم المتحدة وفي المنظمات الإقليمية الأخرى – بتعزيز معايير سلوك الدول في الفضاء السيبراني، وفي الالتزام بالقانون الدولي القائم، وتدابير بناء الثقة (CBMs) في الفضاء السيبراني. ومع ذلك، فإن التعاون في هذه المواضيع مع منطقة الشرق الأوسط وشمال أفريقيا يبدو غائباً إلى حدّ كبير، وينبغي تدعيمه لتعزيز رؤية الاتحاد الأوروبي للفضاء السيبراني.

- **دور الجهات الفاعلة غير الحكومية في تعزيز المناعة السيبرانية.** إنّ مشاركة الجهات الفاعلة غير الحكومية – المجتمع المدني والقطاع الخاص – أمر بالغ الأهمية للتحول الرقمي الفعال والمستدام. وعلى الرغم من أنّ تعزيز مشاركة أصحاب الشأن المتعددين في المسائل المتعلقة بالفضاء السيبراني في جميع أنحاء المنطقة قد يساعد في نهاية المطاف على سدّ الخلافات بين المناعة المجتمعية ومناعة الدولة في جميع أنحاء المنطقة، إلّا أنّ بلدان الشرق الأوسط وشمال أفريقيا كانت مترددة في المشاركة في هذا التعاون، وكان الوصول إلى عملية صنع السياسات محدوداً.

وتقدم الدراسة عدداً من التوصيات المتعلقة بالسياسة العامة لتعزيز التعاون بين الاتحاد الأوروبي وشركائه عبر البحر الأبيض المتوسط، على محورين رئيسيين: السياسات العامة، وآليات التعاون.

## السياسات العامة

- تعزيز سياسات الصحة السيبرانية إضافة إلى التوعية السيبرانية في المنطقة من خلال الحملات والتمارين، والتدريبات الإلكترونية، ومسابقات الأمن السيبراني.
- مواصلة حوار سياسي أكثر قوة بين الاتحاد الأوروبي والشركاء في المنطقة فيما يتعلق بمواقفهم بشأن القضايا الدبلوماسية الرئيسية المتعلقة بالفضاء السيبراني، ولا سيما تطبيق القانون الدولي القائم بشأن الفضاء السيبراني، ومعايير السلوك المسؤول للدولة.
- تحديد نوع المناعة التي يجب تعزيزها في المنطقة، مع الأخذ في الاعتبار إمكانية المفاضلة بين مناعة النظام والمناعة المجتمعية.
- تقليل مخاطر استخدام مشاريع بناء القدرات الإلكترونية في التجسس والرقابة وغيرها من قدرات مراقبة المعلومات.
- تعزيز التعاون بين المنظمات الإقليمية لتطوير وتنفيذ تدابير بناء الثقة الخاصة بكل منطقة بهدف إنشاء منطقة فضاء سيبراني منزوعة السلاح.

## آليات التعاون

- إنشاء آليات لجمع البيانات بصورة أفضل من أجل تقييم مخاطر الجرائم السيبرانية في جميع أنحاء المنطقة، بما في ذلك البناء على المشاريع القائمة بالفعل.
- تعزيز المشاركة الشاملة للقطاع الخاص والمجتمع المدني في صياغة السياسات السيبرانية ورصدها. وبهذا المعنى، يتعين على الاتحاد الأوروبي أن يولي اهتماماً وثيقاً وخاصّاً لخلق الفرص والقنوات من أجل مشاركة أكثر شمولاً للأطراف المتعددة من أصحاب الشأن.
- تعزيز قدرات منطقة الشرق الأوسط وشمال أفريقيا من خلال الشبكات القائمة، عبر مجموعة كاملة من المسائل، اعتماداً على قنوات الاتصال القائمة لتبادل وتعزيز المعرفة التقنية داخل المنطقة ومحاكاة الجهود.
- تعزيز التعاون مع البلدان التي لا تزال مترددة بشأن تفضيلاتها السياسية فيما يتعلق بالمعايير الدولية للفضاء السيبراني.

# المقدمة

باتريك باولاك
Patryk Pawlak
مسؤول تنفيذي في بروكسل، معهد
الاتحاد الأوروبي للدراسات الأمنية (EUISS)

يُعَدّ تعزيز مناعة الدولة والمجتمع أحد الأهداف الرئيسية للاستراتيجية العالمية للاتحاد الأوروبي التي تنعكس في السياسات الموضوعية والإقليمية للاتحاد. ويشمل ذلك أيضاً التعاون في قضايا مثل الأمن السيبراني والجرائم السيبرانية مع دول في منطقة الشرق الأوسط وشمال أفريقيا (MENA). ونظراً لأن عدداً متزايداً من الدول الشريكة تشرع في عملية التحول الرقمي أو تستثمر فيها، فإن الخبرة الجماعية للاتحاد الأوروبي في هذا المجال – على مستوى الاتحاد الأوروبي والدول الأعضاء – يمكن أن تكون ذات قيمة للبلدان التي غالباً ما تواجه نفس التحديات والخيارات المتعلقة بالسياسات العامة.

وإدراكاً لمستويات التنمية الاقتصادية المختلفة، ومراعاة للتكوين المؤسسي أو التنظيمي أو المجتمعي لكلٍّ منها، يمكن للاتحاد الأوروبي أن يكون شريكاً مهمّاً للبلدان في منطقة الشرق الأوسط وشمال أفريقيا، وأن يقدم الدعم اللازم في عملية التحول نحو **مجتمعات رقمية تتمتع بالمرونة والمناعة السيبرانية، وتقوم على احترام القوانين والحقوق.** وفي الوقت نفسه، يُعَدّ التعاون مع دول الشرق الأوسط وشمال أفريقيا بشأن المناعة السيبرانية، والجرائم السيبرانية، والاقتصاد الرقمي والسلوك المسؤول في الفضاء السيبراني، أمراً بالغ الأهمية لتحقيق الهدف المشترك المتمثل في الفضاء السيبراني الحرّ والمفتوح والآمن والمستقر. وتهدف أجندة جديدة للبحر الأبيض المتوسط تم الكشف عنها في فبراير 2021 إلى "تحقيق تعافٍ بيئي ورقمي مرن وعادل" استناداً إلى افتراض أنّ "الازدهار المستدام والمناعة لا يمكن بناؤهما إلّا من خلال شراكة قوية عبر البحر الأبيض المتوسط".

إنّ المنطقة تمزقها الفروق ومدى التفاوت فيما يتعلق بمستوى الرقمنة والربط الشبكي (World Bank, 2014). ووفقاً لمؤشر الاتصال العالمي للهاتف المحمول التابع للنظام العالمي للاتصالات المتنقلة (GSMA)، فإن الدول التي سجلت أعلى الدرجات في المنطقة هي إسرائيل والكويت وقطر والمملكة العربية السعودية والإمارات العربية المتحدة. وشهدت العديد من البلدان الأخرى في جنوب البحر الأبيض المتوسط نموًا مرتفعًا أيضاً في الاتصال بين عامي 2014 و 2018، بما في ذلك تونس والمغرب وتركيا (GSMA, 2019). كانت أسباب تخلف المنطقة في تطوير شبكات النطاق العريض، والوصول إلى الإنترنت واستخدامها، وإنشاء المحتوى الرقمي، هيكلية في جزء منها (البنية التحتية والتكلفة والتنظيم)، وسياسية في جزء منها أيضاً، فالنخب السياسية في جميع أنحاء المنطقة تخشى أن يؤدي إضفاء الطابع الديمقراطي على الوصول إلى الإنترنت إلى تقويض سيطرة الدولة على المعلومات (HRW, 1999). وقد انعكس هذا الاتجاه في العقد الماضي بعد الضغط من مجتمعات الأعمال والبحوث التي شددت على قيمة التحول الرقمي في عملية النمو الاقتصادي، والتنافسية والتحول الديمقراطي في بلدانها. ومع تحسن الاتصال عبر المنطقة، تستثمر الحكومات في تطوير قدراتها، وتشارك العديد من البلدان بنشاط في المناقشات الدولية الجارية حول السلوك المسؤول في الفضاء السيبراني (مثل مصر والأردن والمغرب وتونس)، أو مستقبل التعاون الدولي في مجال مكافحة الجرائم السيبرانية (مثل الأردن ولبنان والمغرب وتونس).

ومع ذلك، فإنّ هذه الإجراءات معرضة لنفس القوى كما هو الحال في بقية العالم، فهناك: الجرائم السيبرانية، والهجمات على البنية التحتية الحيوية (CI)، والأنشطة الخبيثة من قبل الجهات الفاعلة الحكومية وغير الحكومية، فضلاً عن الانتهاكات المحتملة للحريات المدنية وحقوق الإنسان كنتيجة لسياسات الدولة العامة السيئة التخطيط. ومع ذلك، **فإن الوضع في المنطقة حساس بشكل خاص بالنظر إلى الطبيعة الهشّة للعمليات الانتقالية: الرقمية والاقتصادية والسياسية والمجتمعية التي تمر بها هذه البلدان. قد**

**يؤدي فشل الحوكمة في الفضاء السيبراني في منطقة الشرق الأوسط وشمال أفريقيا إلى تقويض هذه الجهود والمساهمة في المزيد من عدم الاستقرار.** وقد يؤدي عدم وجود تشريعات كافية ومؤسسات قوية لضمان التشغيل الآمن للبنية التحتية الحيوية إلى فشلها، وإبطاء التحول الاقتصادي، وزيادة حدة التحديات الإدارية، وتقوية المشاعر المناهضة للحكومة، مما يؤدي إلى الاضطرابات الاجتماعية. وحتى الجهود المتصورة للتلاعب بالعمليات الانتخابية في المنطقة أو التأثير عليها، أو السياسات الحكومية التي تفرض قيوداً على حقوق المواطنين عبر الإنترنت قد تقوض شرعية مثل هذه العمليات وتغذي الاستياء. وأخيراً، فإنّ الاهتمام الاستراتيجي بجنوب البحر الأبيض المتوسط الذي أظهره اللاعبون الإقليميون والخارجيون الآخرون – من خلال زيادة وجودهم الاقتصادي، أو الاستثمار في البنية التحتية أو حتى العمليات السيبرانية التي ترعاها الدولة – يزيد من هذا التعقيد. وبالتالي، فإنّ تعاون الاتحاد الأوروبي مع دول الشرق الأوسط وشمال أفريقيا لا بدّ أن يتم بناؤه من خلال التعرف على هذه الحقائق والديناميّات المختلفة.

# المصادر و المراجع

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSMA). (2019). Mobile Internet connectivity 2019. Middle East and North Africa factsheet. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/ 2019/09/Mobile-Internet-Connectivity-MENA-Fact-Sheet.pdf

HUMAN RIGHTS WATCH (HRW). (1999). The Internet in the Middle East and North Africa: a cautious start. In The Internet in the Mideast and North Africa: free expression and censorship. Retrieved from https://www.hrw.org/legacy/ advocacy/internet/mena/int-mena.htm

WORLD BANK. (2014). Broadband networks in the Middle East and North Africa: key facts. Retrieved from https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/MNA_Broadband_Key_Facts_English.pdf

# الاقتصاد الرقمي والجرائم السيبرانية

**ألكسندرا ماريون يمنى لبن**
**Alexandra Marion Youmna Laban**
مديرة مشروع، المؤسسة الفرنسية
للإنجاز والدراسات والاستشارات (SOFRECO)

# المقدمة

يُعَدّ الوصول إلى الاقتصاد الرقمي – من حيث البنية التحتية وأدوات السياسة العامة – شرطاً أساسيّاً لجني فوائده الاقتصادية والإنمائية. وتعتبر منطقة الشرق الأوسط وشمال أفريقيا (MENA) مؤهلة لتصبح قوة اقتصادية رقمية (UNESCWA, 2019a) نظراً لعدد سكانها البالغ 400 مليون نسمة، والقوى العاملة المتعلمة والشابة، وإمكانية الوصول إلى الموارد الطبيعية، واللغة المتجانسة نسبيّاً، والموقع الجغرافي المتميز. وإبتداءً من أبريل 2019، بلغ انتشار الإنترنت في منطقة الشرق الأوسط وشمال أفريقيا 67,2٪ (Statista, 2019) أكثر من الضعف مقارنة بعقد مضى. بالإضافة إلى ذلك، حقق الاقتصاد الرقمي والثورة الصناعية الرابعة في منطقة الشرق الأوسط وشمال أفريقيا قفزة في الإنتاجية مع التوسع في استخدام الروبوتات المتقدمة وتقنيات التصنيع.

ومع ذلك، فإن اعتماد جزء لا يستهان به من الاقتصاد على المنصات القائمة على الإنترنت يترافق مع أنواع جديدة من النشاط الإجرامي الذي انتشر في هذا القطاع الاقتصادي الجديد. وعلى الرغم من عدم وجود تعريف متفق عليه عالميّاً للجريمة السيبرانية، لأغراض هذا الفصل، تشير الجريمة السيبرانية إلى الأنشطة الإجرامية التي تشارك فيها أجهزة الكمبيوتر وأنظمة المعلومات، إما كأداة أساسية أو كهدف أساسي (EU Cyber Direct, 2020). وتعيق هذه الجرائم النمو الاقتصادي عبر الإنترنت، حيث تكلف حوالي 530 مليار يورو على مستوى العالم (Latici, 2019)، بينما تهدد أمن المواطنين والشركات والدول وتزرع عدم الثقة في الخدمات الرقمية. وبطبيعتها، تُعَدّ الجرائم السيبرانية تحدياً عابراً للحدود، ويُعتبَر التعاون الدولي ضروريّاً لاحتواء نمو النشاط الإجرامي غير المنضبط، وكذلك التشريعات المحلية الرادعة، والقدرات المُعزِّزة للتعرف على مجرمي الإنترنت ومقاضاتهم (EU Cyber Direct, 2020).

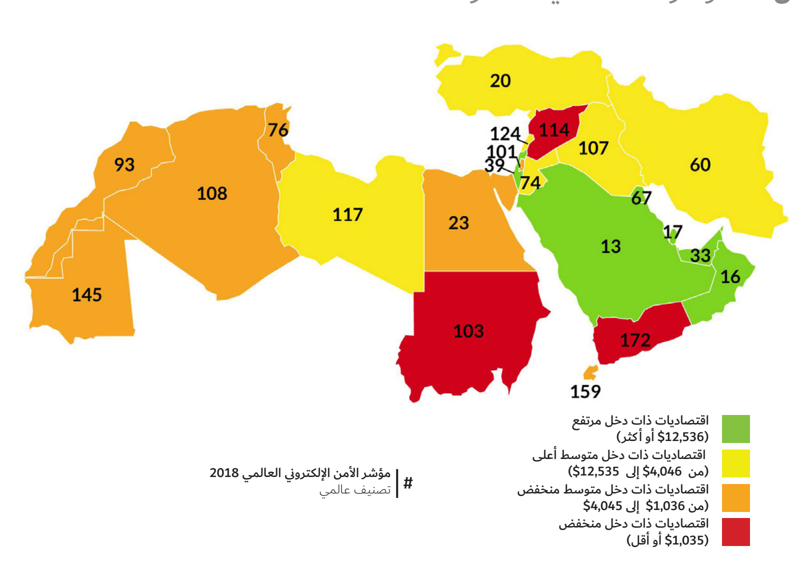
يبحث هذا الفصل في تطور الجريمة السيبرانية وتأثيرها في منطقة الشرق الأوسط وشمال أفريقيا، هذه المنطقة التي تكيفت بشكل مثير للإعجاب مع التقنيات الجديدة، وأصبحت – في الوقت نفسه – مُعرَّضة لجرائم جديدة بنفس الطريقة التي تُرتَكب بها في أجزاء أخرى من العالم. وعلى الرغم من التباين فيما يتعلق بالتعرض للجرائم السيبرانية والنضج للتعامل مع هذا التحدي في أنحاء المنطقة، يقدم هذا الفصل بعض الاستنتاجات فيما يتعلق بأنشطة التعاون السابقة والجارية في مجال الجرائم السيبرانية في منطقة الشرق الأوسط وشمال أفريقيا، والممولة من قبل الاتحاد الأوروبي، وعلى وجه الخصوص أداة الجوار والشراكة الأوروبية (V. Spidiron, C-PROC, personal communication, November 20, 2020; M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020). وبينما ينصب التركيز الأساسي في هذا الفصل على الجزائر ولبنان والمغرب، تشارك دول أخرى في منطقة الشرق الأوسط وشمال أفريقيا أيضاً في نشاط في مكافحة الجرائم السيبرانية، بما في ذلك الأردن وتونس ودول مجلس التعاون الخليجي (GCC). وهناك أربع توصيات سياساتية تستهدف صانعي السياسة العامة على المستوى الوطني، وعلى مستوى الاتحاد الأوروبي يُختتَم بها الفصل، وهي تقدم معلومات عن الخطوات التالية للتعاون بين الاتحاد الأوروبي والشرق الأوسط وشمال أفريقيا في مجال مكافحة الجرائم السيبرانية. وتستند استنتاجات هذا الفصل إلى مقابلات أجريت مع الخبراء بين نوفمبر 2020 وفبراير 2021.

يضعف الاستقرار الإقليمي بسبب غياب الهياكل والمؤسسات الأمنية، الأمر الذي يهدد بدوره بجعل منطقة الشرق الأوسط وشمال أفريقيا عرضة للصراع الدائم، بما في ذلك في الفضاء السيبراني.

## الجريمة السيبرانية: عائق أمام النمو وتهديد للاستقرار

تُعرَّف التنمية الاقتصادية عموماً بأنها العملية التي تُحسِّن الرفاه الاقتصادي للمنطقة، ونوعية الحياة من خلال توفير مستويات معيشية عالية وتوظيف عالي الجودة. ويُعَدّ تطوير اقتصاد منطقة الشرق الأوسط وشمال أفريقيا أحد الشروط الأساسية لاستقرارها. فهو يجمع بلداناً مختلفة وذات تباين شديد من حيث الاقتصاد والأمن السيبراني (انظر الشكل 1 أدناه) وقد عانت، لعقود من الزمان، من تعاقب الأنظمة الاستبدادية، ومعدلات بطالة مرتفعة بين الشباب والنساء، ومستويات عالية من التوظيف الحكومي، والدعم الحكومي الكبير للسلع، والتضخم المالي، والاعتماد على عائدات الريع المتقلبة (سلع النفط والغاز، وكذلك السياحة وتحويلات المغتربين) (Gaub, 2019; Belhaj, 2021). وفوق هذا الوضع الاجتماعي الاقتصادي القاتم نجد حالة مزمنة من الاضطرابات الاجتماعية والعنف، تتجسد في الطائفية والصراعات المستمرة، والهجرة غير النظامية، والتطرف، والمشتريات الضخمة للأسلحة، والمنافسات الجيوسياسية، والاعتماد المفرط على قمع الدولة (Youssef et al., 2020). وإلى جانب ذلك، يضعف الاستقرار الإقليمي بسبب غياب الهياكل والمؤسسات الأمنية، الأمر الذي يهدد بدوره بجعل منطقة الشرق الأوسط وشمال أفريقيا عرضة للصراع الدائم، بما في ذلك في الفضاء السيبراني.

**الشكل 1 :** مؤشرات اقتصادية مختارة.




المصدر: World Bank (2019); ITU (2018).

في عام 2017، اعتبرت النسخة غير السرية من الأداة الأورومتوسطية لتقييم التهديدات (EMTA) الجريمة السيبرانية تهديداً متزايداً، وقد ورد ذلك في تحليلها للجريمة المُنظَّمة الخطيرة، والأنشطة الإرهابية في المنطقة الأورومتوسطية (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020). تاريخيّاً، كانت منطقة الشرق الأوسط وشمال أفريقيا هدفًا لهجمات متطورة، ويتضح ذلك من خلال البرمجية التجسسية شمعون المنسوبة لإيران، وهي التي هاجمت أرامكو في السعودية في أغسطس 2012 (Shires & Hakmeh, 2020). يمكن اعتبار العمليات السيبرانية التي ترعاها

الدولة أنشطة إجرامية، الأمر الذي يؤدي إلى عدم الوضوح في الخطوط الفاصلة بين إنفاذ القانون والاستجابات الاستخباراتية في الفضاء السيبراني. تتعدد أمثلة الجرائم السيبرانية في المنطقة. وتشير الأداة الأورومتوسطية لتقييم التهديدات إلى "الاتحاد الإلكتروني الإسلامي المغربي" (CIVIPOL & Euromed Police IV, 2017) الذي نشط حتى مارس 2018 كمثال على استخدام المنظمات الإرهابية لتكنولوجيا المعلومات والاتصالات (ICT) لشن هجمات سيبرانية (TRAC, n.d.). ومن الأمثلة على المُنظَّمة الناشطة في مجال القرصنة فريق فالاجا التونسي الذي قام بتشويه 33605 موقع إلكتروني حول العالم، وخاصّة في فرنسا، حيث قام عناصر الفريق بتشويه العديد من مواقع الوزارات (Zone-H, n.d.). ومثال آخر على النشاط المعقد لمجرمي الإنترنت في منطقة الشرق الأوسط وشمال أفريقيا هو حملة التجسس الإلكتروني الكبرى، التي أطلق عليها اسم "دارك كاراكال" (Dark Caracal)، والتي تمت تغطيتها أيضاً في فصل بولاك في هذه الدراسة. استهدفت هذه الحملة آلاف الأفراد في 21 دولة وتعمل من مبنى وكالة الاستخبارات اللبنانية منذ يناير 2012 (SMEX, 2018). وبالتالي، فإنّ التصدي لخطر الجريمة كمُسَعِّر للصراع وعدم الاستقرار هو أمر بالغ الأهمية في منطقة الشرق الأوسط وشمال أفريقيا.

تمتد الصلة بين الجريمة والصراع بشكل واضح إلى الفضاء السيبراني، ويخلق عدم الاستقرار مساحة وفرصة لازدهار الأنشطة الإجرامية (الاتّجار غير المشروع بالموارد الطبيعية، والرسوم والرشاوى، والاتّجار غير المشروع بالمخدرات، ونهب الآثار وبيعها)، بينما تؤدي الجريمة المُنظَّمة أيضاً إلى استمرار الصراع من خلال توفير وسائل مربحة لشنّ نزاعات أطول (Steenkamp, 2017). هذه الارتباطات تصبح أسهل باعتبار أنّ الوصول إلى تكنولوجيا المعلومات والاتصالات يوسّع ويُضخّم طبيعة الجريمة العابرة للحدود. وعلى هذا النحو، يستخدم المجرمون الأدوات الإلكترونية للتواصل، وجمع الأموال، وتنسيق الأنشطة غير المشروعة بطريقة أسهل وأسرع وأكثر أماناً، وتبقى مجهولة الهوية. وقد أصبح هذا الارتباط واضحاً بشكل خاص في سياق الاستخدام الإرهابي للإنترنت. إنّ السمات السياسية الرئيسية للمنطقة، أي الأنظمة الانتقالية والصراعات الأهلية والطائفية، تضع أسسًا مواتية للإرهاب المحلي والعابر للحدود، "مما يجعل هذه المنطقة بؤرة الإرهاب العالمي" (Kim & Sandler, 2020). وعلى الرغم من أنها ليست ظاهرة جديدة تماماً (UNODC, 2013)، فإن المنظمات الإرهابية في منطقة الشرق الأوسط وشمال أفريقيا تستخدم استراتيجيات وتكتيكات مجرمي الإنترنت ونشطاء القرصنة عبر الإنترنت لتُلهم وتتواصل وتجند وتدرب وتتبادل أخبار النجاح والفشل وتدعو إلى القيام بأنشطة إرهابية (Vacca, 2020, p. 54). وتعتمد الأخيرة أيضاً على العديد من مصادر الدخل، وتستخدم مجموعة من الأساليب الإلكترونية لجمع الأموال، مثل وسائل التواصل الاجتماعي ومنصات التمويل الجماعي والعملات الافتراضية، وغيرها من الأساليب (FATF, 2015). وقد أصبح هذا تحدياً كبيراً بشكل خاص في أعقاب الصراع في سوريا عندما استخدم تنظيم الدولة الإسلامية في العراق والشام المعروف بتنظيم داعش (ISIS) وسائل التواصل الاجتماعي والفضاء السيبراني كإحدى قنوات نشاطه الرئيسية، إضافة إلى قنوات إعلامية متطورة (Berton & Pawlak, 2015).

وعلاوة على ذلك، تتيح هذه الأدوات الإلكترونية توسيع نطاق أنشطة التخريب والتجسس في المنطقة، حيث تفسح شبكة مُعقّدة من الجهات الفاعلة – بدءًا من الدول المعادية إلى شبكات الجريمة المُنظَّمة، والمنظمات الإرهابية، والجهات الفاعلة غير الحكومية – تفسح الطريق في هذا المجال الجديد لزعزعة الاستقرار، وتشويه سمعة المنظمات العامة والخاصة، انظر أيضاً (Pawlak's chapter and the Abdel-Sadek's Annex of this study). وتتراوح الأنشطة من اعتراض البيانات غير القانوني، إلى التنصت غير

القانوني، وتخريب البيانات والنظم، وإساءة استخدام الأجهزة، وعمليات التزوير والاحتيال المرتبطة بالكمبيوتر، والمواد الإباحية المتعلقة بالأطفال، ومخالفة حقوق النشر وحقوق الجوار (CIVIPOL & Euromed Police IV, 2017). ويساهم انخفاض مستوى الصحة السيبرانية عبر المنطقة في زيادة تعرض المنطقة للجرائم السيبرانية (CIVIPOL & Euromed Police IV, 2017). وتتضمن الأساليب الشائعة المستخدمة في الهجمات السيبرانية استغلال المعلومات لارتكاب جرائم، مثل التجسس، وانتحال صفة الأشخاص للحصول على خدمات البضائع أو المال أو التواصل مع أشخاص آخرين، وارتكاب الاحتيال الطبي والسرقة، وتحقيق الدخل من بيانات الشركات أو الحكومات أو من بيانات الرعاية الصحية الحساسة (Vacca, 2020, p. 21). ولكن يبقى هناك المزيد من هذه الأساليب، إذ يمكن استخدام خدمات الصرف النقدي لشراء الهواتف المحمولة بطريقة غير مشروعة، وبالتالي التحايل على القوانين التي تُلزِم مستخدمي بطاقة SIM بتقديم الهوية عند التسجيل؛ وهذه الهواتف المحمولة غير المسجلة هي باب للجرائم السيبرانية. ويعمل نشطاء القرصنة الإقليميون في المنطقة، ويرتكبون جرائم ذات تأثير محدود مثل تشويه المواقع الإلكترونية. وتُعتبَر البرمجيات الخبيثة كخدمة هي النشاط الإجرامي الأكثر انتشاراً في المنطقة من حيث الجرائم السيبرانية التي تم الإبلاغ عنها. ويُعتبر التصيّد الاحتيالي أيضاً جزءًا أساسيّاً من الاحتيال في جميع أنحاء المنطقة، حيث تمكّن اللغة المشتركة المجرمين من الوصول إلى الضحايا عبر الحدود الوطنية. وهناك العديد من أنواع أنشطة التصيّد الاحتيالي، مثل الاحتيال المالي، وسرقة البيانات الشخصية، والتسويق غير القانوني عبر الإنترنت، والاحتيال الرومانسي، وهجمات الدخلاء والوسطاء (man-in-the-middle) والابتزاز الجنسي (CIVIPOL & Euromed Police IV, 2017).

## الجهود المحلية لمكافحة الجريمة السيبرانية

تستهدف الهجمات السيبرانية بلدان الشرق الأوسط وشمال أفريقيا أكثر من بقية العالم بنسبة 6٪، وتُعتبر المنطقة "واحدة من أكثر مناطق العالم استهدافاً من حيث الجرائم السيبرانية وفقدان البيانات" (Gonçalves, 2019). وعلى سبيل المثال، تحدثت تقارير عن الإمارات العربية المتحدة (UAE) باعتبارها ثاني أكثر دولة مُستهدَفة في العالم من حيث الجرائم السيبرانية، حيث تكلف هذه الجرائم الدولة ما يقدر بنحو 1,15 مليار يورو سنويّاً، إذ استغل مجرمو الإنترنت جائحة كورونا لصالحهم أيضاً (UNODC, 2020). أبلغ مركز ميميكاست لتهديدات الاستخبارات (Mimecast Threat Intelligence Center) عن زيادة بنسبة 751٪ في عدد النقرات غير الآمنة خلال الأشهر الثلاثة الأولى من عام 2020 في منطقة الشرق الأوسط وشمال أفريقيا (Bell, 2020). وفي حين أنّ المعلومات الإحصائية حول الجرائم السيبرانية في جميع أنحاء المنطقة لا تزال تمثل تحدياً، فإنّ هناك بعض الجهود لمعالجة هذه الفجوة. وقد نشرت الوكالة الوطنية التونسية لأمن الحاسوب منذ عام 2018 إحصاءات الفضاء السيبراني التونسي، وهي تُظهر ارتفاعاً سنويّاً في انتهاكات الأمن السيبراني المكتشَفة، حسب النوع (ANSI, 2020).

تستهدف الهجمات السيبرانية بلدان الشرق الأوسط وشمال أفريقيا أكثر من بقية العالم بنسبة 6٪، وتُعتبر المنطقة "واحدة من أكثر مناطق العالم استهدافاً من حيث الجرائم السيبرانية وفقدان البيانات

ترتبط هذه الاتجاهات بعدد متزايد من التحقيقات المتعلقة بالجرائم السيبرانية عبر دول الشرق الأوسط وشمال أفريقيا، مما يدل على مشاركة صانعي السياسات العامة الإقليميين في إيجاد حلول مناسبة لهذا التهديد الجديد (CIVIPOL & Euromed Police IV, 2017). ويهدف صانعو السياسات العامة الوطنيين إلى إعداد أو تحديث إطار الحوكمة السيبرانية المعمول به حالياً من أجل محاسبة ومحاكمة هذه الجرائم الجديدة وفقاً لذلك. وفي السنوات الخمس الماضية، برز اكتشاف الجرائم السيبرانية وتعطيلها في جدول أعمال السياسات العامة، ويرجع ذلك جزئيّاً إلى إنشاء هياكل محددة لإنفاذ القانون.

تتضمن المعركة الفعالة ضد الجرائم السيبرانية عدداً كبيراً من الولايات، وتتطلب التكيف المستمر لصانعي السياسات العامة ووكالات إنفاذ القانون (LEAs) مع مشهد التهديد المتطور. ولكن لا يمكن لأي حكومة أن تفعل ذلك بمفردها، مما يجعل التعاون مع القطاع الخاص والمنظمات غير الحكومية (NGOs) مكوناً رئيسيّاً في التنفيذ الناجح لأية استراتيجية لمكافحة الجرائم السيبرانية. ويساعد هذا التعاون أيضاً على تجنب الازدواجية والتكرار اللذين لا داعي لهما من خلال تركيز الجهود وضمان التشاور الواسع مع جميع أصحاب الشأن: الموظفين القضائيين، وموظفي قطاع تكنولوجيا المعلومات والاتصالات، ومسؤولي الدفاع والشرطة، وفرق الاقتصاد والمنظمات غير الحكومية، والقطاع الخاص.

وفي الوقت نفسه، يساعد نهج "المجتمع بأسره" تجاه الأمن السيبراني أيضاً في تعزيز نهج محوره الإنسان، من خلال تقليل مخاطر الانتهاكات المحتملة لحقوق الإنسان وتعزيز سيادة القانون. ولهذا أهمية خاصة لأن مراقبة محتوى الوسائط الاجتماعية والتحكم فيه أصبح جانبًا رئيسيّاً للسياسة العامة للأمن السيبراني في منطقة الشرق الأوسط وشمال أفريقيا، مما يضر أحياناً بحرية التعبير عبر الإنترنت، كما هو موضح بمزيد من التفصيل في ملحق عادل عبد الصادق لهذه الدراسة. وتحت غطاء السيطرة على انتشار الدعاية الراديكالية (المتطرفة) على الإنترنت، قامت العديد من حكومات الشرق الأوسط وشمال أفريقيا بتقييد الحريات المدنية على الإنترنت والحدّ من حرية التعبير. **يرى هذا الفصل أنّ السياسات العامة السيبرانية يجب أن تساهم بقدر كبير في تدعيم حقوق الإنسان وسيادة القانون، والحكم الديمقراطي، والتنمية البشرية، من أجل ضمان الأمن والثقة في تكنولوجيا المعلومات والاتصالات.**

## الجزائر

شهدت الجزائر مستوى كبيراً من إضفاء الطابع المؤسساتي على مكافحة الجرائم السيبرانية. وهناك تركيز تدريجي على الكفاءة داخل وزارة الدفاع الوطني (MND). وقد تمّ في السابق تكليف إدارة المخابرات والأمن بالمراقبة الإلكترونية من خلال مجموعة التحكم في الشبكة. وكانت الهيئة الوطنية للوقاية من الجرائم المُتَّصلة بتكنولوجيا المعلومات والاتصال ومكافحتها (ONPLCILTIC) تابعة لوزارة العدل حتى يوليو 2019، عندما تم تحويلها إلى وزارة الدفاع الوطني. ومع ذلك، فإن مراقبة الجرائم السيبرانية والإبلاغ عنها تقع تحت مسؤولية مركز منع ومكافحة جرائم الكمبيوتر والجرائم السيبرانية (CPLCIC) التابع لقيادة الدرك الوطني، أو تحت مسؤولية خلايا الأمن السيبراني التابعة للمديرية العامة للأمن القومي (DGSN). ووفقاً للإحصاءات الرسمية، عالج أكثر من 3000 قضية متعلقة بالأمن السيبراني في عام 2018 (Kahlane, 2019, p. 13).

ومع ذلك، يتفق الخبراء على ثلاثة أوجه قصور في النظام الحالي:

أولاً، لم يكتمل النظام المعياري والتنظيمي بعد، كما أنّ إنشاء هيئات مراقبة الجرائم السيبرانية المنصوص عليها في النصوص يتم ببطء. ثانياً، هناك نقص في الموارد اللوجستية والبشرية لتحسين هذا الإطار المؤسسي الجديد. ثالثًا، الميل إلى المركزية المفرطة في الاستجابة للجرائم السيبرانية يعيق التكامل مع القطاع الخاص والمجتمع المدني اللذين من شأنهما توفير الموارد والدعم للإدارة فيما يتعلق بهذه القضايا (S. Bechiri, Realistic Security, personal communication, December 8, 2020).

اكتسبت الجزائر تدريجياً وسائل مكافحة الجريمة السيبرانية منذ عام 1997، ووفقاً لمجلس أوروبا (CoE)، فإنّ الترسانة القانونية المعمول بها تجعل من الممكن مكافحة معظم جرائم الكمبيوتر المذكورة في اتفاقية بودابست بشأن جرائم الإنترنت. ولا تزال مواطن الضعف قائمة في مجالات القانون الإجرائي والتعاون الدولي. ولا يوجد حاليّاً أي جهة وطنية مسؤولة عن حماية نظم المعلومات ورفع مستوى الوعي حول هذا الموضوع، على الرغم من أنّ الافتقار إلى أمن تكنولوجيا المعلومات يمثل مشكلة كبيرة للبلاد. وقد صدر مرسوم رئاسي بتاريخ 20 يناير 2020 بهدف معالجة بعض أوجه القصور التي تم تحديدها سابقاً فقط، من خلال وضع إطار عمل لأمن نظم المعلومات الوطنية الذي ينص على إنشاء ثلاث منظمات لتطوير استراتيجية أمن نظم المعلومات الوطنية وتنسيق تنفيذها. وسيتألف هذا الهيكل المؤسساتي من كيانات جديدة، تحت إشراف وزارة الدفاع الوطني تضمّ: المجلس الوطني لأمن نظم المعلومات، ووكالة أمن أنظمة الكمبيوتر، وأول فريق وطني للاستجابة للطوارئ الحاسوبية (CERT)، أي المركز التشغيلي الوطني لأمن الكمبيوتر. كما ينصّ على أنه يجب على جميع الكيانات العامة والخاصة تعيين كبير مسؤولي أمن المعلومات (Bechiri, 2020).

بدأت مجموعات العمل الأولى المسؤولة عن تنفيذ هذا الإصلاح المؤسسي عملها، لكنّ تقدّمها تُعيقه القيود المتعلقة بجائحة كورونا. وسيساهم هذا الهيكل بمجرد إنشائه في توفير المزيد من الوضوح بشأن الحوكمة السيبرانية في الجزائر، حيث سيجمع العديد من الجهات الفاعلة تحت مظلة واحدة، لأنّه صاحب الشأن الحكومي الرئيسي للمشاركة في مجال مكافحة الجرائم السيبرانية.

## لبنان

يسجل لبنان مستويات منخفضة إلى حدّ ما في المؤشرات الدولية، فيما يتعلق بمستويات الاتصال والأمن السيبراني (انظر الشكل 1 أعلاه). وصاحب الشأن الرئيسي في مكافحة الجرائم السيبرانية هو مكتب مكافحة جرائم المعلوماتيّة وحقوق الملكية الفردية المثير للجدل، والتابع للشرطة القضائية داخل قوى الأمن الداخلي، وقد تأسس في عام 2006 لتعزيز الأمن على الإنترنت ومكافحة الجريمة السيبرانية. ويركز المكتب على معالجة سرقة الهوية، وغسيل الأموال، والمواد الإباحية المتعلقة بالأطفال، فضلاً عن شكاوى التشهير والقذف والقدح عبر الإنترنت. وله دور مزدوج يتمثل في التحقيق في الشكاوى وخروقات الأمن السيبراني، والجرائم المتعلقة بالتكنولوجيا، تحت إشراف السلطات القضائية، مع توفير الوعي الأساسي للمؤسسات العامة والتعليمية بشأن أحدث التهديدات السيبرانية. وقد استُخدِم مكتب مكافحة جرائم المعلوماتية كأداة إكراه لتنظيم وإزالة الخطاب غير المواتي من وسائل التواصل الاجتماعي (Quino, 2015). كما عززت مؤسسات ووكالات حكومية أخرى، مثل الجيش والأمن العام وأمن الدولة، قدراتها التحقيقية لمنع التهديدات للأمن القومي، بما في ذلك الهجمات السيبرانية والتجسس الإلكتروني.

خلُصت اللجنة الوطنية للأمن السيبراني في يوليو 2019 إلى أنّ الخطوة الحاسمة الوحيدة لبدء استراتيجية الأمن السيبراني اللبنانية هي إنشاء وكالة وطنية لنظام معلومات الأمن السيبراني (NCISA) لتقييم نقاط الضعف، وللتوصية بالتدابير الوقائية، وتحديد التهديدات، والاستجابة للهجمات على الفور وبكفاءة، والحفاظ على الأمن (Araz, 2019). ومن المتوقع أن تسهل هذه الوكالة التنسيق بين مختلف الجهات الفاعلة، وأن تسهل أيضاً النهج الاستباقي لإدارة قضايا الأمن السيبراني، مع تتبع نمو وتنوع التهديدات

السيبرانية ومعالجة تطورها. وستكون الوكالة الوطنية لنظام معلومات الأمن السيبراني مسؤولة مباشرة أمام رئيس مجلس الوزراء، وستلحق بالأمانة العامة لمجلس الدفاع الأعلى. وتفترض استراتيجية الأمن السيبراني أيضاً إنشاء فريق الاستجابة لحوادث الأمن السيبراني (CSIRT) كسجل مركزي للحوادث السيبرانية لدعم المعالجة والدفاع والوقاية من الهجمات المُخطَر عنها. ولا يوجد حاليّاً فريق وطني للاستجابة للطوارئ الحاسوبية (N. Alkhatib, Bank Audi, personal communication, February 12, 2021; S. Araz, Middle East Institute, personal communication, February 12, 2021).

## المغرب

حقق المغرب تميزاً قانونياً وتقنياً في مكافحة الجرائم السيبرانية. ومع ذلك، لا تزال الترسانة التنظيمية مقصورة على المنظمات الحيوية، وتتجاهل معظم القطاع الخاص (DATAPROTECT & AUSIM, 2018). اعتمد البرلمان المغربي مشروع القانون 20-05 المتعلق بالأمن السيبراني في 14 يوليو 2020. ويمثل هذا القانون خطوة مهمة نحو تعزيز القدرات الوطنية في مجال الأمن السيبراني، وتوسيع نطاق أمن نظم المعلومات من خلال دمج الفئات النشطة الأخرى، مثل الجمهور من مشغلي شبكات الاتصالات، ومقدمي خدمات الأمن السيبراني، وموفّري الخدمات الرقمية. ويهدف إلى وضع إطار لتبادل البيانات، والتعاون بين الهيئة الوطنية للأمن السيبراني والأجهزة المختصة لمكافحة الجرائم السيبرانية وإساءة استخدام البيانات الشخصية، وأخيراً يوفر في المحصلة أرضية قانونية للتعاون الدولي في مجال الأمن السيبراني (Moroccan Parliament, 2020).

وقد حظيت هذه الجهود بتقدير من مجلس أوروبا الذي يعتمد على المغرب في دعم نشر ترسانة قانونية مُحدَّثة قادرة على التصدي للجرائم السيبرانية في منطقة الشرق الأوسط وشمال أفريقيا في إطار مشروعيها: الإجراء العالمي بشأن الجرائم السيبرانية+ (GLACY+) ومشروع سايبر ساوث (CyberSouth). ويمكن في المغرب حاليّاً تقديم شكوى ضد أي جريمة سيبرانية إلى الفريق المغربي للاستجابة للطوارئ الحاسوبية (maCERT)، وهو مركز للكشف عن هجمات الكمبيوتر ولاتخاذ إجراءات بصددها، وهو جزء من إدارة الدفاع الوطني والمديرية العامة لأمن نظم المعلومات. ويتيح مكتب المساعدة التابع للفريق المغربي للاستجابة للطوارئ الحاسوبية لأي مواطن الإبلاغ عن حادثة عبر الإنترنت، من خلال استكمال نموذج الإبلاغ عن الحادث وإرساله بالبريد الإلكتروني أو الفاكس. ولدى الفريق المغربي للاستجابة للطوارئ الحاسوبية خط ساخن أيضاً. ومع ذلك، يتخلف المغرب عن الركب فيما يتعلق بهياكله التنظيمية، لعدم وجود استراتيجية مُحدَّثة للأمن السيبراني، والفشل في مراقبة المؤشرات الإحصائية، وهي عيوب رئيسية في كفاءة نظام مكافحة الجرائم السيبرانية. وعلاوة على ذلك، يستعرض ملحق الدراسة الذي أعدّه عادل عبد الصادق التطورات القائمة في المغرب من منظور انفتاح الإنترنت، وحرية التعبير والوصول.

# العملية الإقليمية لمكافحة الجريمة السيبرانية

اتخذت البلدان في جميع أنحاء المنطقة خطوات لتعزيز تعاونها ضد الجرائم السيبرانية على المستوى الإقليمي، بالتزامن مع الجهود الوطنية. وتُعَدّ اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية – المعروفة أيضاً باسم اتفاقية مالابو (MC) والمؤرخة في 27 يونيو 2014 – أكثر الجهود شمولاً في هذا الصدد. ومع ذلك، لم

تحظَ الاتفاقية بتأييد واسع، وتواجه مشاكل في التصديق بين الدول الأعضاء في مُفوَّضية الاتحاد الأفريقي (O. Daas, AFRIPOL, personal communication, November) (AU 18, 2020)؛ ففي منطقة الشرق الأوسط وشمال أفريقيا، وقعت عليها دولتان فقط هما: موريتانيا في فبراير 2015، وتونس في أبريل 2019. وتركز اتفاقية مالابو على الجوانب الفنية للأمن السيبراني، بينما تظل مسألة الأدلة الإلكترونية في القضايا القانونية دون حلّ. لذلك يُعَدّ التعديل ضرورياً لإنشاء بوابة لإدارة الأدلة، وإرساء أساس للتفعيل في مجال الجرائم الإلكترونية، على قاعدة مبدأ التعاون بين البلدان الأفريقية.

وتنشط منظمة الشرطة الجنائية الأفريقية (الأفريبول) (AFRIPOL) التي أُطلقت في عام 2015، في مجال التعاون في مكافحة الجرائم السيبرانية. في عام 2018، وبدأت مجموعة عمل معنية بالجرائم السيبرانية تجتمع مرتين في السنة بهدف تطوير استراتيجية إقليمية لمكافحة الجريمة السيبرانية. والهدف من هذه الوثيقة هو وضع إطار إقليمي للأدوات المستخدمة (المعدات والإجراءات)، وتدريب خبراء الشرطة، ووضع الإطار القانوني والتشريعي لإعداد اتفاقية فيما يخص الجرائم السيبرانية. وتنبع الحاجة إلى استراتيجية إقليمية لمكافحة الجريمة السيبرانية من ملاحظة أنّ القارة الأفريقية متباينة من حيث التقدم، فضلاً عن التباين في المعايير والأدوات. واستعداداً للاستراتيجية الإقليمية، تم إجراء دراسة في 55 دولة، وتُعتبر دول شمال أفريقيا من بين أكثر الدول تقدماً في هذا المجال. وفي الواقع، ستتم دعوة الجزائر لتدريب خبراء جرائم الإنترنت من الدول الأعضاء في الاتحاد الإفريقي. وتتمثل الخطوات التالية في المصادقة المستمرة على الاستراتيجية، وتوفير الأدوات من قبل راع واحد أو أكثر لقوات الشرطة غير المجهزة، والتدريب في مراكز الامتياز الإقليمية (رواندا وجنوب أفريقيا والسنغال)، والاستفادة من برنامج دعم الإنتربول للاتحاد الأفريقي (ISPA) بشأن الأفريبول الذي انطلق في 28 أبريل 2020، وخاصّة فيما يتعلق ببناء القدرات العملياتية في مجال الجرائم السيبرانية. أمّا مشاريع الشراكة الأخرى فهي قيد التطوير حاليّاً، ولا سيّما مع وكالة تطبيق القانون الأوروبية (يوروبول) (EUROPOL)، ووكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون (CEPOL). والجرائم السيبرانية هي أحد الموضوعات التي يتم تناولها.

تشمل الصكوك والاتفاقيات الإقليمية الأخرى في منطقة الشرق الأوسط وشمال أفريقيا الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات الصادرة عن جامعة الدول العربية (2010)، والاستراتيجية العربية للبحث العلمي والابتكار من قبل المُنظَّمة العربية للتربية والثقافة والعلوم (ALECSO, 2014)، والمبادرة العربية الإقليمية بشأن الثقة والأمن في استخدام الاتصالات وتكنولوجيا المعلومات والاتصالات، وشبكة مركز التميز للاتحاد الدولي للاتصالات في المنطقة العربية من 2015 إلى 2018 (UNESCWA, 2019a).

## الشرق الأوسط وشمال أفريقيا والتعاون الدولي في مكافحة الجريمة السيبرانية

تشارك دول الشرق الأوسط وشمال أفريقيا أيضاً في الجهود الدولية لمكافحة الجريمة السيبرانية من خلال كلٍّ من الاتفاقيات العالمية الحالية، مثل اتفاقية بودابست بشأن جرائم الإنترنت، ومن خلال الجهود الجارية المبذولة في الأمم المتحدة (UN) عبر مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) في فيينا، وفي اللجنة الثالثة بمقر الأمم المتحدة في نيويورك.
كانت اتفاقية بودابست لعام 2001 هي المعاهدة الدولية الأكثر صلة التي تسعى إلى التصدي للجرائم السيبرانية من خلال مواءمة القوانين الوطنية، وتحسين تقنيات

تُعَدّ اتفاقية بودابست الاتفاقية القانونية الوحيدة الملزِمة التي توفر إطاراً للتعاون الدولي في مكافحة الجرائم السيبرانية

التحقيق، وزيادة التعاون بين الدول. وتُعَدّ اتفاقية بودابست الاتفاقية القانونية الوحيدة الملزِمة التي توفر إطاراً للتعاون الدولي في مكافحة الجرائم السيبرانية، وقد كانت بمثابة معيارٍ أساسي لوضع بقية المعايير الدولية في هذا المجال (Pawlak, 2017). وحددت اتفاقية بودابست إعطاء الأولوية للجرائم السيبرانية في التعاون الدولي. ودخلت حيز التنفيذ في يوليو 2004، وتضم 65 طرفًا و 9 دول في طور الانضمام حتى لحظة كتابة هذا التقرير. وتتطلب عملية الانضمام إجراء تقييم من مجلس أوروبا، ومن لجنة اتفاقية الجرائم السيبرانية (T-CY)، يؤدي إلى مواءمة التشريعات اللازمة وتحديثها، وبعد ذلك تتم دعوة الدولة للانضمام لتصبح عضوة في الاتفاقية. إنّ الميزة الرئيسية للتصديق على اتفاقية بودابست هي أنها تسمح للمؤسسات المحلية بالتفاعل مع البلدان الأخرى بشكل أكثر سلاسة. وقد أصبح المغرب طرفًا كاملاً في المعاهدة في 26 يونيو 2018 بفضل مشاركته المبكرة في التعاون في مجال مكافحة الجرائم السيبرانية.

ودعيت تونس أيضاً للانضمام إلى اتفاقية بودابست في 13 فبراير 2018، لكنها لم تصبح طرفًا كامل العضوية، إذ لا يزال مشروع قانون مواءمة التشريعات الوطنية مع أحكام اتفاقية بودابست ينتظر الموافقة. والسلطات التونسية لديها القدرات اللازمة لمكافحة الجريمة السيبرانية والتعامل مع الأدلة الإلكترونية، ويساعد مشروع سايبر ساوث السلطات التونسية بشكل أكبر في مجال التدريب القضائي، والمبادئ التوجيهية للتعامل مع الأدلة الإلكترونية (V. Spiridon, C-PROC, personal communication, November 20, 2020).

وفيما يتعلق بالتشريعات الدولية الإضافية حول الجرائم السيبرانية، نشرت لجنة اتفاقية الجرائم السيبرانية 11 مذكرة إرشادية تعمل كآلية متابعة لتوضيح اتفاقية بودابست للأطراف بشكل أفضل، وتقديم تعريفات تكميلية (T-CY, 2012). ويجري حالياً إعداد البروتوكول الإضافي الثاني لاتفاقية بودابست من قبل لجنة اتفاقية الجرائم السيبرانية. وتشمل العناصر الإضافية التعاون الدولي المُعَزّز بين السلطات العامة والقطاع الخاص، وسلطات تحقيق جديدة للوصول إلى البيانات، ومناقشة الأدلة الإلكترونية للاتحاد الأوروبي (T-CY, 2020).

وعلى الرغم من أنّ الانضمام إلى اتفاقية بودابست مفتوح لجميع البلدان، فإنّ الاتفاقية لم تكتسب اعترافاً عالميّاً كاتفاقية ملزمة على المستوى الدولي. وقد واجهت معارضة قوية من بعض الدول على نحو خاصّ، ولا سيما روسيا التي تُعَدّ المؤيد الرئيسي لإصدار معاهدة دولية جديدة بشأن الجرائم السيبرانية تحت رعاية الأمم المتحدة (Hakmeh & Peters, 2020). وفي عام 2019، اقترح قرار رعته روسيا إنشاء لجنة خبراء مخصَّصة للعمل من أجل معاهدة جديدة للأمم المتحدة. وشاركت عدة دول في منطقة الشرق الأوسط وشمال أفريقيا مثل الجزائر وإيران وليبيا والسودان وسوريا في رعاية القرار، وصوَّت 15 آخرون لصالحه، وصوتت دولة واحدة فقط ضدّه (إسرائيل)، وامتنعت ستّ دول عن التصويت (البحرين، جيبوتي، المغرب، المملكة العربية السعودية، تونس وتركيا) (UN, 2019). انعقدت الجلسة التنظيمية للجنة المُخصَّصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية في الفترة من 10 إلى 12 مايو 2021. وأثناء مناقشة التأجيل، شاركت بلدان منطقة الشرق الأوسط وشمال أفريقيا بنشاط، حيث قامت المملكة العربية السعودية وسوريا بمراقبة العملية عن كثب، وقدمت مصر الآراء ووجهات النظر. وتمّ في الاجتماع انتخاب السفيرة فوزية بومعيزة مباركي من الجزائر رئيسة للمجموعة، وأصبح السفير محمد حمدي الملا من مصر أحد نواب الرئيس الثلاثة عشر. ويشير الخبراء إلى وجود تباين سياسي استراتيجي

بين السياسيين الذين يتخذون قراراتهم على أساس التوافق الأيديولوجي، والعاملين على الأرض (مثل وكالات إنفاذ القانون الذين لا يزالون يستفيدون بشكل مباشر من الدعم الممول من الاتحاد الأوروبي في معالجة الجرائم السيبرانية (V. Spidiron, C-PROC, personal communication, November 20, 2020; M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020).

أخيراً، تمَّ في 12 نوفمبر 2018 دعم نداء باريس للثقة والأمان في الفضاء السيبراني من قبل الدول والحكومات المحلية والشركات ومنظمات المجتمع المدني (CSOs). ونصّ المبدأ التاسع من هذا النداء على تشجيع القبول والتنفيذ الواسعين للمعايير الدولية للسلوك المسؤول، وتدابير بناء الثقة في الفضاء السيبراني من خلال تسهيل تبادل المعلومات بشأن الجريمة السيبرانية. ودعمت العديد من دول الشرق الأوسط وشمال أفريقيا نداء باريس، وهذه الدول هي الكويت ولبنان والمغرب وقطر وتونس والإمارات العربية المتحدة (Paris Call, 2018).

## دور الاتحاد الأوروبي في دعم دول الشرق الأوسط وشمال أفريقيا

حددت *استراتيجية الاتحاد الأمني للاتحاد الأوروبي 2020–2025* الأمن السيبراني بوصفه مسألة ذات أهمية استراتيجية. وتوصَف التبعية للإنترنت، وظهور الجرائم السيبرانية، والسرقة الإلكترونية للأسرار التجارية بأنها أسباب منطقية لاتخاذ خطوات على الأرض. وتعتبر استراتيجية الاتحاد الأوروبي للأمن السيبراني لعام 2013 "الحد بشكل كبير من الجرائم السيبرانية" أحد أولوياتها الخمس. وفي هذا الصدد، تشمل الأولويات الخارجية للاتحاد الأوروبي تعزيز الحوار بين الاتحاد الأوروبي والدول الشريكة على مستوى أصحاب الشأن المتعددين، وتعزيز العلاقات مع الشركاء المتشابهين في التفكير بما يخص الجرائم السيبرانية، والاستفادة من الخبرة الأوروبية في المسائل المتعلقة بالإنترنت.

على الرغم من عدم ذكر منطقة الشرق الأوسط وشمال أفريقيا بشكل صريح، كان الاتحاد الأوروبي شريكاً رئيسيّاً في دعم المنطقة في مكافحتها للجرائم السيبرانية، وقام – بالتالي – بتمويل العديد من الإجراءات في هذا الصدد. والسبب الأساسي لهذه المشاركة هو دعم شركاء الجوار الجنوبي (SN) في جهودهم للانضمام إلى حوار أصحاب الشأن المتعددين حول الجرائم السيبرانية من خلال الاستفادة من خبرة الاتحاد الأوروبي. وعلى الرغم من عدم ذكر الجريمة السيبرانية رسميّاً في برامج العمل لسنوات متعددة وكذلك في برامج العمل السنوية في سياسة الجوار الأوروبية – دول الجنوب (ENP)، فإنّ بعض الأنشطة في مجال بناء قدرات الأمن السيبراني تتم في إطار مشاريع المساعدة الفنية الوطنية واتفاقيات الشراكة، أو يتم دعمها من مبادرات الاتحاد الأوروبي العالمية الأخرى التي يمولها الاتحاد الأوروبي.

## مشروع يوروميد للشرطة 4

بدأ التعاون الإقليمي بشأن الجرائم السيبرانية بين الاتحاد الأوروبي ومنطقة الشرق الأوسط وشمال أفريقيا من خلال مشروع يوروميد للشرطة 4 (Euromed Police IV)، وهو جزء من الشراكة الأورومتوسطية

وفقاً للخبير الذي تمت استشارته، بدأ التعاون الإقليمي بشأن الجرائم السيبرانية بين الاتحاد الأوروبي ومنطقة الشرق الأوسط وشمال أفريقيا من خلال مشروع يوروميد للشرطة 4 (Euromed Police IV)، وهو جزء من الشراكة الأورومتوسطية (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020). وقد تم تمويل هذا المشروع من قبل المديرية العامة للمفوضية الأوروبية لمفاوضات الجوار والتوسع، وتم تنفيذه من فبراير 2016 إلى يناير 2020 من قبل اتحاد مشترَك عام – خاص يضم سبع دول أعضاء في الاتحاد الأوروبي، وهي: فرنسا، ألمانيا، إيطاليا، هولندا، رومانيا وسلوفينيا. وكان هدف المشروع هو دعم وكالات إنفاذ القانون (الشرطة والدرك) لدول الجوار الجنوبي في الاتحاد الأوروبي: الجزائر ومصر وإسرائيل والأردن ولبنان والمغرب وفلسطين وتونس. واستُبعِدت ليبيا وسوريا لأسباب أمنية. تمّ تحديد خمسة مجالات للجريمة بعد التشاور بين الاتحاد الأوروبي والمستفيدين، وتمّ تطوير مصفوفة مفصلة لظواهر الجريمة في المنطقة. وهذه الظواهر هي: الإرهاب، والجريمة السيبرانية، والاتجار بالبشر، والاستغلال الجنسي، والهجرة، والمخدرات، والأسلحة والمتفجرات.

كانت الجريمة السيبرانية على رأس جدول الأعمال، مع ثلاث أولويات فرعية وأنشطتها المشتقة منها:

الأول هو تعزيز قدرة قوات الأمن وفرق التحقيق في استخدامها لشبكات الإنترنت والشركات المزودة للوصول إلى شبكة الإنترنت. وكدليل على نجاح هذا النشاط، عُقِد في الجزائر العاصمة اجتماع أولي بين الشركات المزودة للوصول إلى شبكة الإنترنت وخدمات التحقيق في الأفريبول، بحضور مزودي خدمة الإنترنت (ISPs) (فيسبوك وجوجل وغيرهما)، وضباط مكافحة الإرهاب، وفرق التحقيق في المنطقة. وكان الهدف هو الشروع في آلية رد فعل فوري عند حدوث تهديد إلكتروني على الشبكات لتسهيل تبادل الاتصال التلقائي، وتعزيز ردود فعل السلطات تجاه الجاني. وهذه الآلية مستخدمة بالفعل في أوروبا، ولم يتم اعتمادها بعد في منطقة الشرق الأوسط وشمال أفريقيا (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020).

وكان المجال الثاني ذو الأولوية هو تعزيز القدرة على مكافحة الجرائم السيبرانية المالية، ومكافحة استغلال الأطفال في المواد الإباحية على الإنترنت. ولم تكن أجهزة الأمن في الجوار الجنوبي مجهزة لمواجهة هذه التهديدات الجديدة. وعُقِد العديد من ورش العمل التدريبية في تونس والمغرب لضباط الشرطة حول أدوات التحقيق على الشبكة المظلمة، وحول أدوات التحقيق في الشرطة والاستخبارات وعملاء مكافحة الإرهاب.

أمّا المجال الثالث ضمن هذه الأولويات فهو تعزيز التعاون الشرطي والقضائي بشأن قضايا الجرائم السيبرانية مع مشروع العدالة الأورومتوسطية من خلال تطوير جميع المتطلبات الأساسية للتحقيقات الجنائية. ونتج عن ذلك إصدار مشترك بعنوان "*كتيب الدليل الرقمي*" في عام 2017، وقد تمّ تناوله لاحقاً ونشره في جميع أنحاء العالم (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020).

كان للمشروع، بشكل عام، تأثير إيجابي على قدرة المنطقة على مكافحة الجريمة السيبرانية. وقد وفر منصة للاتصال وجهاً لوجه بين القطاع الخاص ووكالات إنفاذ

القانون لدعم التعاون في المنطقة، من أجل تحسين فهم التحديات الرئيسية للجرائم السيبرانية من خلال ورش العمل حول الشبكة المظلمة ومواضيع أخرى، ولنشر *كتيب الدليل الرقمي*. ونتج عن المشروع أيضاً نجاح إنشاء شبكتين لوكالات إنفاذ القانون، لا تزالان نشطتين حتى الآن، على الرغم من وجود القليل من الاستجابات حاليّاً فيما يخص أنشطة الجرائم السيبرانية، وهاتان الشبكتان هما: شبكة التحليل، حيث يقوم كلّ بلد من دول الجوار الجنوبي بتغذية المعلومات الاستراتيجية وغير التشغيلية إلى اليوروبول من خلال قاعدة بيانات أورومتوسطية؛ والشبكة المتخصصة في بناء القدرات التي تتعامل مع الجريمة القائمة.

بالمقارنة مع الأولويات الأخرى للمشروع، كان التعاون في مجال مكافحة الجرائم السيبرانية هو المجال الذي ميّز التعاون بين الاتحاد الأوروبي ودول الشرق الأوسط وشمال أفريقيا. وتَمثَّل أحد محاور التعاون المشجعة في تعزيز الروابط بين الجهات الفاعلة العامة والخاصة في مجال الجرائم السيبرانية من خلال المساهمة في تطوير أساليب تحقيق مُوحَّدة في مكافحة استغلال الأطفال في المواد الإباحية. وهناك حاجة لاتخاذ إجراءات إضافية في المستقبل، إذ قد لا يتم إضفاء الطابع المؤسساتي الكامل على بعض الأنشطة التي نُفِّذَت. ولدى الوحدات المعنية في وزارات الداخلية الآن شبكات إقليمية قوية نسبيّاً.

تم إطلاق مشروع يوروميد للشرطة 5 في أكتوبر 2020، مع وكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون باعتبارها المنفّذ الرئيسي. وقد شاركت وكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون في إنشاء قاعدة المعارف الأورومتوسطية بهدف التحول إلى المركزية في إجراءات التعاون المنفذة في مجال مكافحة الجريمة، ولا سيما الجرائم السيبرانية.

## الإجراء العالمي بشأن الجرائم السيبرانية+ ومشروع سايبر ساوث

بالإضافة إلى ما سبق، قدم الاتحاد الأوروبي الدعم للمشاريع الأخرى التي تركز على الجرائم السيبرانية، والتي تكون عالمية النطاق، ولكنها تشمل بلدان الشرق الأوسط وشمال أفريقيا. وبالتعاون مع مجلس أوروبا، منذ عام 2014، دعم الاتحاد الأوروبي الإجراء العالمي بشأن الجرائم السيبرانية (GLACY)، وتلاه حاليّاً مشروع الإجراء العالمي الموسع بشأن الجرائم السيبرانية أو ما يطلق عليه مشروع الإجراء العالمي بشأن الجرائم السيبرانية+ (V. Spidiron, C-PROC, personal communication, November 20, 2020). والهدف من الإجراء العالمي بشأن الجرائم السيبرانية+ هو تعزيز قدرات 15 دولة ذات أولوية، بما في ذلك المغرب، لتطبيق التشريعات المتعلقة بالجرائم السيبرانية والأدلة الإلكترونية. يدعم الإجراء العالمي بشأن الجرائم السيبرانية+ هذه الدول في أن تصبح محاور إقليمية تقوم بتنفيذ الأنشطة وتبادل الدروس المستفادة. كان المغرب من أوائل الدول الواقعة ضمن سياسة الجوار الأوروبية – دول الجنوب التي تتناول إجراءات الجرائم السيبرانية بشكل فردي. وكدليل على مشاركة المغرب الطويلة في التعاون الدولي بشأن الجرائم السيبرانية، يقود القضاة المغاربة ورش عمل تدريبية في بلدان أخرى (V. Spidiron, C-PROC, personal communication, November 20, 2020).

مشروع سايبر ساوث هو عمل مشترك آخر للاتحاد الأوروبي ومجلس أوروبا بدأ في عام 2017، وله أهداف مماثلة، ولكنّه يستهدف منطقة الشرق الأوسط وشمال أفريقيا على وجه التحديد: الجزائر والأردن والمغرب ولبنان وتونس. والهدف منه هو تعزيز قدرات سلطات العدالة الجنائية بشأن الجرائم السيبرانية، ودعم التشريعات من خلال التدريب

المؤسسي والتعاون بين الوكالات وبين الدول أيضاً (CoE, 2021). والميزة الإقليمية المهمة لهذا المشروع هي الاستفادة من تجربة المغرب في مكافحة الجرائم السيبرانية، حيث إنه البلد الأكثر تقدماً على المستوى الإقليمي. إنّ العمل مع شريك متمرس خاض العملية بالفعل سيمكن الشركاء الآخرين من الاستفادة من نفس المنهجية لتطوير القدرات وأفضل الممارسات، بينما يمكن للشريك الأكثر تقدماً الاستمرار في تلقي الدعم. إنّ النماذج وأفضل الممارسات في تشريعات الأمن السيبراني والأدلة الإلكترونية موجودة، ومع ذلك، يجب التعامل مع الطموحات الإقليمية بحكمة، حيث إنّ السؤال حول مَن يمتلك الدور القيادي هو سؤال حساس (V. Spidiron, C-PROC, personal communication, November 20, 2020).

يتم تنفيذ الأنشطة الرئيسية في تدريبات إنفاذ القانون والقضاء التي يتم إجراؤها في هذه البلدان في مجال التحاليل الجنائية الحاسوبية والاستخبارات مفتوحة المصدر من منظور تدريب المدرِّب، إذ يُجري قضاة مدرَّبون تدريبات للقادمين الجدد، علماً بأنّ المبادئ التوجيهية لتأمين وجمع وتحليل الأدلة الإلكترونية لا تتماشى أو تنسجم مع أفضل الممارسات الدولية، وقد تم تقديم الدعم في هذا الصدد. ومنذ حلقات العمل الأولى التي عقدت لفائدة الهياكل في كل بلد، تم تسجيل تقدم كبير، ووضعت بعض البلدان مبادئ توجيهية محلية للتعامل مع الأدلة الإلكترونية. وتقوم مجموعات العمل المحلية حاليّاً بجهد مشترك لتطوير مواد التدريب الوطنية حول الجرائم السيبرانية في البلدان الخمسة المُستهدَفة (بما في ذلك مناهج معاهد التدريب القضائي). كما تسهل أمانة الشبكة القضائية لبرنامج سايبر ساوث الحوارات بين القضاة في المنطقة حول مواضيع الجرائم السيبرانية والأدلة الإلكترونية، وهي قناة غير رسمية لتعزيز التعاون الدولي.

## الاستنتاجات والتوصيات

وخلاصة القول، تندمج منطقة الشرق الأوسط وشمال أفريقيا تدريجيّاً في الاقتصاد الرقمي العالمي، ولكن – على الرغم من ذلك – هناك حاجة إلى التحول في آلية التفكير نحو تعزيز تنمية قطاع خاص قادر على المنافسة حقاً، وترشيد التوظيف في القطاع العام، وتنويع الاقتصاد أو تحويله إلى اقتصاد آخر يُولِّد النمو، بصرف النظر عن النفط والغاز.

ومن العلامات الواعدة على التنويع الاقتصادي في منطقة الشرق الأوسط وشمال أفريقيا الشهية للتكنولوجيا والابتكار التي بدأت بالظهور؛ ففي الواقع، هناك تحول جارٍ من الاستهلاك السلبي للتكنولوجيا إلى توطينها والاعتماد عليها لأغراض معيّنة (UNESCWA, 2019b). وتُعَدّ تطبيقات نقل الركاب المنتشرة، ومنصة بث الموسيقى الإقليمية أمثلة ونماذج للاعتماد على التكنولوجيا. ومع ذلك، هناك حاجة إلى مزيد من الجهود للتحرك نحو الإنتاج المحلي، ونحو مستويات الابتكار التكنولوجي المطلوبة في الاقتصاد الرقمي.

في منطقة الشرق الأوسط وشمال أفريقيا هناك تحول جارٍ من الاستهلاك السلبي للتكنولوجيا إلى توطينها والاعتماد عليها لأغراض معيّنة

إنّ أحد الجوانب الخفية لهذا الأفق المتفائل هو الضعف الشديد وسوء الصحة السيبرانية في المنطقة في مواجهة المخاطر الجديدة، ولا سيما الاتجاهات الإجرامية الجديدة، إذ ترتكز العديد من الجهات الفاعلة، من الدول المتنافسة إلى الجهات الفاعلة غير الحكومية، والجماعات الإرهابية والمعارضة السياسية، على شبكة الإنترنت، مستغلةً الوصول السهل والسريع والمجهول للقيام بأنشطة غير مشروعة. ويصدق هذا بشكل أكبر في منطقة مستقطَبة ومعرَّضة للحرب، مثل منطقة الشرق الأوسط وشمال أفريقيا.

ظهرت الجريمة السيبرانية بسرعة كواحدة من أخطر التهديدات المجتمعية، وتحدياً رئيسياً لوكالات إنفاذ القانون في المنطقة. وتُعتبَر التجربة الوطنية لاستراتيجية الأمن السيبراني خطوة حاسمة في إنشاء إطار عمل مشترك للاستجابة لهذه المشكلة المتصاعدة.

بُذلت جهود في هذا الاتجاه في منطقة الشرق الأوسط وشمال أفريقيا، وقد ركّز هذا الفصل على تقديم الحلول الإدارية والقانونية المتاحة للمواطنين ضحايا الهجمات السيبرانية في ثلاث دول، وهي الجزائر ولبنان والمغرب، حيث تنشط هذه الدول بشكل خاص في التعاون مع الاتحاد الأوروبي في هذا المجال.

وبالنظر إلى أنّ الجريمة السيبرانية هي قضية عابرة للحدود بطبيعتها، فإنها تتطلب تعاوناً دولياً لتقوية وزيادة تقارب التشريعات الوطنية من أجل تتبع ومقاضاة شبكات المجرمين السيبرانيين عبر الحدود. والمفاوضات الجارية في الأمم المتحدة بشأن التبني المحتمل لمعاهدة جديدة للجرائم السيبرانية تثير الخلاف بين دول العالم، ومنطقة الشرق الأوسط وشمال أفريقيا ليست استثناءً، حيث تدعم غالبية دول الشرق الأوسط وشمال أفريقيا هذه العملية مع توقع أنها ستوفر مزيداً من الوضوح بشأن القواعد المطبقة على الفضاء السيبراني.

وتماشياً مع هدفه المتمثل في تعزيز الحوار بين أصحاب الشأن المتعددين حول الأمن السيبراني، يعمل الاتحاد الأوروبي منذ عام 2014 لدعم دول الجوار الجنوبي في جهودها لتطوير إداراتها وأطرها التشريعية في مكافحة الجريمة السيبرانية. والعديد من المبادرات المُموَّلة من الاتحاد الأوروبي المذكورة في هذا الفصل تتكاتف، من بين عدة أمور أخرى، لدعم البلدان التي ترغب في اعتماد اتفاقية بودابست وتحسين قدرتها على الاستجابة للهجمات السيبرانية. ويرى هذا الفصل أيضاً أنّ الاتحاد الأوروبي شريك شرعي لدعم منطقة الشرق الأوسط وشمال أفريقيا في جهود مكافحة الجرائم السيبرانية بسبب مشاركته المبكرة في العملية، وحرصه المستمر على الدعم، كما يتضح من العديد من المشاريع الجارية المُموَّلة من الاتحاد الأوروبي.

تم اقتراح أربعة تدابير ملموسة كطريق للمضي قدماً، يسترشد بها صُنّاع السياسات العامة على الصعيد الوطني في منطقة الشرق الأوسط وشمال أفريقيا لدفع إصلاح مكافحة الجرائم السيبرانية الذي تشتد الحاجة إليه بدعم من الشركاء الملتزمين مثل الاتحاد الأوروبي.

1. **اعتبار جمع البيانات خطوة ضرورية لتقييم مخاطر الجرائم السيبرانية.** يجب على صانعي السياسات العامة إعطاء الأولوية لحجم تكاليف الجرائم السيبرانية، وأعداد وأنواع الهجمات، والصناعات والإدارات الأكثر تضرراً. وستسلط المعلومات التي يتمّ جمعها الضوء على مدى انتشار الجريمة السيبرانية، وستساعد على تحديد مستويات التهديد المناسبة. ويجب على صانعي السياسات العامة في الاتحاد الأوروبي ودول الشرق الأوسط وشمال أفريقيا الاستفادة من المرحلة الجديدة من البرنامج الإقليمي ميدستات (MEDSTAT) الذي هو حالياً في مرحلة تقديم العطاء، والذي يتمثل هدفه في تنسيق الإحصاءات في سياسة الجوار الأوروبية – دول الجنوب، من خلال إضافة إحصاءات الأمن السيبراني إلى الحقول المستهدفة حالياً.

2. **تعزيز المشاركة الشاملة للقطاع الخاص والمجتمع المدني في صياغة السياسات العامة السيبرانية ورصدها.** يتفق الخبراء الذين تمت استشارتهم على أنّ طريقة

تعزيز التعاون في التصدي للجرائم السيبرانية تتمثل في الانخراط مع القطاع الخاص، ووضع خطط تعاون جديدة، مثل التهجين في توفير الأمن السيبراني، وتوسيع التبعية بين الجهات الفاعلة العامة والخاصة. وتُعَدّ الشراكات بين القطاعين العام والخاص في مكافحة الجريمة السيبرانية عنصراً لا غنى عنه. ويجب تطوير هذا المجال من التعاون. وعلى الرغم من بدء الاتصالات لم يتم إضفاء الطابع المؤسسي عليها حتى الآن. وتوفر المرحلة الجديدة من مشروع يوروميد للشرطة 5 الذي تم إطلاقه مؤخراً، إطاراً مناسبًا لإدخال مشاركة القطاع الخاص والتشاور على نطاق أوسع.

3. **تعزيز قدرات منطقة الشرق الأوسط وشمال أفريقيا من خلال الشبكات القائمة.** قدّم هذا الفصل المشاريع الإقليمية التي أنشأت شبكات ومراكز امتياز، يتفاعل من خلالها موظفو الدولة (وكالات إنفاذ القانون والمدّعون العامّون والقضاة) من جميع أنحاء منطقة الشرق الأوسط وشمال أفريقيا ويشاركون أفضل الممارسات والتطبيقات. وهذا الجهد يُؤتي ثماره، وخاصة أنه يوفر قناة اتصال لتبادل وتعزيز المعرفة داخل المنطقة، والاستفادة من الجهود المشتركة. وتظهر أهمية ذلك بشكل خاص في سياق التجانس اللغوي النسبي لهذه المنطقة.

4. **تعزيز الصحة السيبرانية في منطقة الشرق الأوسط وشمال أفريقيا.** يتمثل أحد العناصر الحاسمة لمنع الجرائم السيبرانية في توعية المستخدِمين بالمخاطر التي يتعرضون لها عبر الإنترنت. وتُبذَل جهود التوعية هذه بالفعل في شكل حملات متعددة تتمثل في تنظيم التدريبات الإلكترونية، ومسابقات الأمن السيبراني، والمشاركة في يوم الإنترنت الآمن، وفعاليات التوعية العامة، مثل أسبوع الأمن السيبراني الإقليمي، وورش العمل المتخصصة الأخرى. ويجب أن تكون هذه الجهود المحلية مستدامة ومنظمة بحيث تلعب المنظمات الإقليمية (لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا، الأفريبول، جامعة الدول العربية) دوراً مُوحَّداً. وبالإضافة إلى جهود بناء القدرات التي يبذلها صانعو السياسات العامة، يمكن لمشاريع سايبر ساوث ويوروميد للشرطة ومشاريع أخرى أن تنفذ أنشطة تعزز المناهج الدراسية في مجال الصحة السيبرانية.

# المصادر والمراجع

AGENCE NATIONALE DE LA SECURITE INFORMATIQUE (ANSI). (2020). Statistiques sur le cyberespace tunisien. Retrieved from https://www.ansi.tn/statistics

ARAZ, S. (2019). Lebanon's cybersecurity strategy emerges. Retrieved from https://mei.edu/publications/lebanons-cybersecurity-strategy-emerges

BECHIRI, S. (2020). Nouvelle organisation de la SSI en Algérie. Retrieved from https://www.realistic-security.com/nouvelle-organisation-de-la-ssi-en-algerie/

BELHAJ, F. (2021). MENA unbound: ten years after the Arab Spring, avoiding another lost decade. Retrieved from https://www.worldbank.org/en/news/ opinion/2021/01/14/mena-unbound-ten-years-after-the-arab-spring-avoiding-another-lost-decade

BELL, J. (2020). Coronavirus: Cybercrime rockets in Middle East as fraudsters exploit COVID-19. Retrieved from https://english.alarabiya.net/News/middle-east/2020/12/07/Coronavirus-Coronavirus-Cybercrime-rockets-in-Middle-East-as-fraudsters-exploit-COVID-19

BERTON, B., & PAWLAK, P. (2015). Cyber Jihadists and their Web. Retrieved from https://www.iss.europa.eu/content/cyber-jihadists-and-their-web CIVIPOL & EUROMED POLICE IV. (2017). Euromed police threat assessment.

COUNCIL OF EUROPE (CoE). (2021). CyberSouth. Retrieved from https://www.coe.int/en/web/cybercrime/cybersouth

CYBERCRIME CONVENTION COMMITTEE (T-CY). (2012). Guidance notes. Retrieved from https://www.coe.int/en/web/cybercrime/guidance-notes

CYBERCRIME CONVENTION COMMITTEE (T-CY). (2020). Protocol negotiations. Retrieved from https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

DATAPROTECT & AUSIM. (2018). Les enjeux de la cybersécurité au Maroc - Livre Blanc. Rabat: Bibliothèque Nationale du Royaume du Maroc.

EU CYBER DIRECT. (2020). Cybercrime at the United Nations Background Note. Retrieved from https://eucyberdirect.eu/wp-content/uploads/2020/06/backgroundnote.pdf

FINANCIAL ACTION TASK FORCE (FATF). (2015). FATF Report. Emerging terrorist financing risks. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

GAUB, F. (2019). Chaillot Paper 154 - Arab futures 2.0 the road to 2030. Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Chaillot_154%20Arab%20Futures.pdf

GONÇALVES, P. (2019). Middle East is the biggest target for cybercrime. Retrieved from https://www.internationalinvestment.net/news/4001693/middle-east-biggest-target-cybercrime

HAKMEH, J., & PETERS, A. (2020). A new UN cybercrime Treaty? the way forward for supporters of an open, free, and secure Internet. Retrieved from https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet

INTERNATIONAL TELECOMMUNICATION UNION (ITU). (2018). Global Cybersecurity Index. Retrieved from https://www.itu.int/pub/D-STR-GCI.01-2018

KAHLANE, A. (2019). La problématique de la concurrence dans le contexte de l'économie numérique. Retrieved from http://www.conseil-concurrence.dz/wp-content/uploads/2019/10/Mr-Kahlane.pdf

KIM, W., & SANDLER, T. (2020). Middle East and North Africa: terrorism and conflicts. Global Policy, 11(4), 424-38.

LATICI, T. (2019). Cyber: how big is the threat? Retrieved from https://www.europarl. europa.eu/ RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

MOROCCAN PARLIAMENT. (2020). La Chambre des Représentants adopte 6 projets de loi relatifs à la défense nationale, à la sécurité informatique et au secteur financier et bancaire. Retrieved from https://www.chambredes-representants.ma/fr/actualites/la-chambre-des-representants-adopte-6-projets-de-loi-relatifs-la-defense-nationale-la

PARIS CALL. (2018). Paris Call for trust in cyberspace. Retrieved from https://pariscall.international/en/call

PAWLAK, P. (2017). A wild wild web? laws, norms, crime and politics in cyberspace. Retrieved from https://www.iss.europa.eu/content/wild-wild-web-law-norms-crime-and-politics-cyberspace

QUINO, Z. (2015). #HackingTeam leaks: Lebanon's cybercrime bureau exploited angry birds to surveil citizens' mobile devices. Retrieved from https://smex.org/ hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

SHIRES, J., & HAKMEH, J. (2020). Briefing - is the GCC cyber resilient? Retrieved from https://www.chathamhouse.org/2020/03/gcc-cyber-resilient

SMEX. (2018). Beirut-based global cyber-espionage campaign a threat to local freedoms. Retrieved from https://smex.org/beirut-based-global-cyber-espionage-campaign-a-threat-to-local-freedoms/

STATISTA RESEARCH DEPARTMENT. (2019). Internet penetration rate in the Middle East and globally 2009-2019. Retrieved from https://www.statista.com/statistics/265171/comparison-of-global-and-middle-eastern-internet-penetration-rate/

STEENKAMP, C. (2017). The crime-conflict nexus and the civil war in Syria. Stability: International Journal of Security & Development, 1, 1-18.

TERRORISM RESEARCH AND ANALYSIS CONSORTIUM (TRAC). (n.d.). Moroc can Islamic Union-Mail. Retrieved from https://www.trackingterrorism.org/ group/moroc%C2%ADcan-islamic-union-mail

UNITED NATIONS ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (UNESCWA). (2019a). Arab horizon 2030 - digital technologies for development. Retrieved from https://www.unescwa.org/publications/arab-horizon-2030-digital-technologies-development

UNITED NATIONS ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (UNESCWA). (2019b). Fourth industrial revolution - impact of the fourth industrial revolution on development in the arab region. Retrieved from https://www.unescwa.org/sites/www.unescwa.org/files/publications/files/impact-fourth-industrial-revolution-development-arab-region-english.pdf

UNITED NATIONS (UN). (2019). Countering the use of information and communications technologies for criminal purposes: resolution adopted by the General Assembly. Retrieved from https://digitallibrary.un.org/record/3841023?ln=en

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). (2013). Comprehensive study on cybercrime. Retrieved from https://www.unodc.

org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). (2020). COVID-19 cyber threat analysis UNODC MENA assessment & actions. Retrieved from https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf

VACCA, J. (Ed.). (2020). Online terrorist propaganda, recruitment, and radialization. Boca Raton, FL, United States: Taylor & Francis Group.

WORLD BANK. (2019). World Bank data. Retrieved from https://datahelpdesk.worldbank.org /knowledgebase/articles/906519-world-bank-country-and-lending-groups

YOUSSEF, T. M., ABOUELDAHAB, N., ABDEL GHAFAR, A., ZOUBIR, Y., FATHOLLAH-NEJAD, A., & KABBANI, N. (2020). Op-Ed The Middle East and North Africa over the next decade: Key challenges and policy options. Retrieved from https://www.brookings.edu/opinions/the-middle-east-and-north-africa-over-the-next-decade-key-challenges-and-policy-options/

ZONE-H. (n.d.). Unrestricted information. Retrieved from http://www.zone-h.org/archive/notifier=Fallaga%20Team/page=50

# الاستقرار وإدارة الإنترنت والمعلومات المُضلِّلَة

صامويل دومينيوني
**Samuele Dominioni**
زميل باحث، المعهد الإيطالي
للدراسات السياسية الدولية (ISPI)

## المقدمة

كان لانتشار تكنولوجيا المعلومات والاتصالات (ICT) آثار ثورية على المجتمعات المعاصرة. وقد وصف لوتشيانو فلوريدي هذا العصر الجديد من الاعتماد على التقنيات الرقمية بأنه "التاريخ المفرط" أو (المتغيّر بسرعة) (Floridi, 2012). وتؤثر هذه التحولات الكبيرة على السياسة أيضاً، إذ تنتشر بالفعل الآثار الإيجابية والسلبية للتقنيات الرقمية؛ فعلى سبيل المثال، يمكن لوسائل التواصل الاجتماعي أن تساعد الناس على إسماع أصواتهم، ومشاركة أحداث الفساد السياسي، أو الممارسات الخاطئة. وفي الوقت نفسه، تعمل تكنولوجيا المعلومات والاتصالات على تضخيم تأثير الأخبار المُزيَّفة وحملات المعلومات المُضلِّلة. كان هناك عدد متزايد من الدراسات التي تبحث في آثار التقنيات الرقمية على السياسة في الديمقراطيات الليبرالية (Deibert, 2019; Bartlett, 2018; Kavanagh & Rich, 2018; Nemitz, 2018) والأنظمة غير الديمقراطية (Dominioni, 2020a; Keremoğlu & Weidmann, 2020; Xu, 2020; Rød & Weidmann, 2015; Deibert et al., 2008; Kalathil & Boas, 2003). ومع ذلك، وكما تشير جاكلين كير (2018)، فإنّ ما لم يحظَ باهتمام كبير حتى الآن هو كيف أنّ التحكم في الإنترنت يمكن أن يؤثر على التطورات الأوسع للأنظمة السياسية.

يهدف هذا الفصل إلى معالجة هذه الفجوة من خلال النظر في ثلاث دول على وجه الخصوص: مصر والأردن والمغرب. وقد شهدت جميع هذه البلدان في العقد الماضي تغييراً دستوريّاً أو إصلاحات، مدفوعة بثورة في مصر، أو بتنازلات من النُّخَب الحاكمة في الأردن والمغرب (Bank & Edel, 2015). وتتمتع جميع هذه البلدان أيضاً بنسبة عالية نسبيّاً من السكان الشباب (حوالي ثلث إجمالي السكان)[1]، ولديها مستويات عالية من الإلمام بالقراءة والكتابة[2]. وبالإضافة إلى ذلك، فإنّ هذه البلدان هي أعضاء – أو كانت في الماضي – أعضاء في منتديات دولية تتناول معايير السلوك المسؤول للدولة في الفضاء السيبراني، مثل فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي (UN GGE)، وفريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي (UN OEWG). وجميع هذه البلدان جزء من سياسة الجوار الأوروبية أيضاً (ENP)، وقد ضمَّنت منذ عام 2017 الأمن السيبراني على وجه التحديد ضمن إجراءاتها (Lannon, 2019). وأخيراً، لا يمكن أن نعتبر أنّ أيّاً من هذه الدول تملك نظاماً ديمقراطيّاً؛ فوفقاً لمؤشر الديمقراطية 2019، تعدّ كلٌّ من مصر والأردن "نظامين استبداديين"، في حين أنّ المغرب "نظام هجين". وتُعتبَر هذه التصنيفات مهمة بقدر ما تسمح بدراسة نماذج حوكمة الإنترنت في الديمقراطيات الليبرالية غير الغربية. وهذا بدوره يثير أسئلة ذات صلة فيما يتعلق بتأثير الإنترنت على استقرار هذه الأنظمة.

الحُجّة هنا هي أنّ السياسات والممارسات المختلفة حول إدارة الإنترنت، ولا سيما تلك المتعلقة بتنظيم المحتوى والمعلومات المُضلِّلة، قد تلعب في الواقع دوراً مهمّاً في تطوير النظام. ونظراً لأنّ المجال الرقمي أصبح أداةً للطعن في هياكل السلطة الحالية والحكام (Bunce & Wolchik, 2010; Eltantawy & Wiest, 2011) أو أصبح "تكنولوجيا تساعد

1) مصر 33,6٪؛ الأردن 33,1٪؛ المغرب 27٪ (CIA World Factbook, 2020).

2) مصر 93,29٪؛ الأردن 99,23٪ ؛ المغرب 95,07٪ (World Data Atlas, 2015).

الشعوب على التحرّر" (Plattner & Diamond, 2012)، يبدو أنه من المبرر إدراج قانون وطني حول الفضاء السيبراني كمتغير يؤثر في القدرة التنظيمية للدولة التي تُعَرَّف بأنها" حدود وتماسك الدولة مع هياكل الحزب الحاكم" (Levitsky & Way, 2010) أو "جهاز قسري قوي و / أو منظمة حزبية" (Levitsky & Way, 2010, p. 25). وبالتالي، فإنّ القدرة التنظيمية القوية هي المفتاح لمواجهة كلٍّ من حالتَي عدم اليقين: المؤسساتية والمعلوماتية، واللتين – كما يرى أندرياس شيدلر (2013) – هما المتغيران الرئيسيان اللذان يلعبان دوراً جوهرياً في الاستقرار الاستبدادي. لذلك، غالباً ما تفشل الاحتجاجات الجماهيرية، والتنافس على الانتخابات في الأنظمة ذات الفجوات المعلوماتية الأقل، كما حدث – على سبيل المثال – مع الدول التي انضمت مؤخراً إلى الربيع العربي (Bank & Edel, 2015). ومع ظهور التقنيات الرقمية، كان على الأنظمة غير الديمقراطية تطوير قدراتها من أجل مواجهة التهديدات والتحديات القادمة من الفضاء السيبراني (Deibert et al., 2010).

وإلى جانب السيطرة الاستبدادية لكبح المعارضة المدنية والسياسية، بذلت العديد من البلدان حول العالم جهوداً لإنشاء تشريعات بشأن الوسائط الرقمية من أجل مواجهة الظواهر الصعبة المتعلقة بالتضليل، مثل التطرف (على سبيل المثال في سياق تنظيم دولة العراق الإسلامية والشام المعروف بتنظيم داعش [ISIS])، والعمليات الإعلامية للتأثير على الانتخابات (مثل الانتخابات الرئاسية الأمريكية لعام 2016). وأثارت هذه الحالات – وخصوصاً في الديمقراطيات الليبرالية – الجدل حول الشروط التي يمكن – ويجب – تقييد حرية التعبير في ظلّها. وأدى تفشي جائحة كورونا إلى زيادة كبيرة في مستوى الاهتمام السياسي بالتضليل كظاهرة عالمية، ممّا فاقم من ضرورة مواجهة الاضطراب المعلوماتي، ودَفَع الأمم المتحدة (UN) إلى إعلان عن "وباء معلوماتي".

ومع تبني العديد من الحكومات في جميع أنحاء العالم سياسات للحدّ من المعلومات المُضلِّلة، بما في ذلك دول الاتحاد الأوروبي، ومنطقة الشرق الأوسط وشمال أفريقيا (MENA)، فإن دراسة العلاقة الثلاثية بين القلق الأمني المشروع، وحماية حقوق الإنسان عبر الإنترنت، واستقرار الأنظمة، يجب أن تصبح أولوية؛ فما هو تأثير هذه السياسات على الحرية والمناعة المجتمعية واستقرار النظام؟ وكيف يمكن التوفيق بين هذه الأهداف المتضاربة أحياناً، وتوفير أرضية مثمرة لتعاون الاتحاد الأوروبي مع دول منطقة الشرق الأوسط وشمال أفريقيا؟

يناقش هذا الفصل نماذج حوكمة الإنترنت في المغرب والأردن ومصر من أجل استخلاص استنتاجات حول كيفية إساءة استخدام النماذج المختلفة لسياسات التحكم في المعلومات. ومن أجل تقييم فرص التعاون بين الاتحاد الأوروبي ودول المنطقة، يقارن الفصل استجابة الاتحاد الأوروبي للأخبار المُزيَّفة والمعلومات المُضلِّلة والتهديدات الإعلامية الأخرى في الدول الأعضاء بتلك الموجودة في المنطقة. ويعتمد التحليل المقدم في هذا الفصل على المقابلات شبه المُنظَّمة مع خبراء في الموضوع، وتحليل أنماط التصويت في الأمم المتحدة، وتحليل المصادر الثانوية مثل التقارير والدراسات المتعلقة بالحريات عبر الإنترنت. وبالنظر إلى الاهتمام الخاص الذي يوليه الاتحاد الأوروبي لبرامج بناء القدرات السيبرانية، يُختَتم الفصل بتوصيات حول كيفية الاستفادة بشكل أفضل من الممارسات الجيدة في هذه البرامج في جميع أنحاء المنطقة.

## مفتوح ومجاني وآمن؟ حوكمة الإنترنت في منطقة الشرق الأوسط وشمال أفريقيا

غالباً ما تتخذ الأنظمة غير الديمقراطية مناهج مختلفة بخصوص الفضاء السيبراني عن تلك الموجودة في الديمقراطيات الليبرالية، ومن ضمنِها المنتديات الدولية التي تحدد القواعد وسلوكيات الدولة في الفضاء السيبراني. ويمكن إرجاع هذا النمط إلى أواخر التسعينيات، عندما أثارت روسيا مسألة مواجهة التهديدات من الفضاء السيبراني في الأمم المتحدة. وأثار طلب فتح نقاش دولي حول التهديدات المعلوماتية انجرافاً بين جبهتين، وهو ما يعكس بشكل متوقع المواقف الجيوسياسية (Dominioni & Rugge, 2020). تنتمي جميع تلك الدول التي أرادت الحفاظ على المبادئ التأسيسية للفضاء السيبراني إلى الجبهة الأولى المسماة "العولمة"؛ وتستند المبادئ التأسيسية إلى النموذج الأساسي لـ "مساحة غير مجزأة" دون حدود، مع تدفق حرّ للمعلومات (Mueller, 2017). وضمّت الجبهة الثانية البلدان التي تصور الفضاء السيبراني، وبالتالي الإنترنت، على أنه مجرد وسيط آخر مثل التلفزيون أو الراديو، وبالتالي كان لا بدّ من التحكم به، وخصوصاً فيما يتعلق بالمحتوى. يشار إلى هذا النهج الثاني باسم "الاتساق" أو "النموذج التوافقي" الذي يعتمد على المواءمة (Mueller, 2017)[3]. وهذان السببان المتضاربان هما أيضاً العاملان الرئيسيان في الإجراءين اللذين دفعا المناقشات في الأمم المتحدة، وأول هذين الإجراءين هو تشكيل فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي، والثاني هو تشكيل فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. ومن المفترض أنّ نجاح وفشل أحدهما يعتمد على التطورات في الآخر (Broeders, 2019).

يتولىّ كلٌّ من المغرب والأردن مراقبة المحتوى على المستوى المحلي، من خلال مزيج من التدابير الرسمية وغير الرسمية

وتسلط الأقسام التالية الضوء على نماذج حوكمة الإنترنت المعتمدة في مصر والأردن والمغرب. وبشكل عام، يمكن الادعاء أنه فيما يتعلق بنماذج حوكمة الإنترنت، تقوم البلدان الثلاثة التي هي موضوع الدراسة بتنفيذ خيارات وممارسات سياسية تتماشى بشكل أكبر مع نهج نموذج "الاتساق" (التوافقي). ويتضح هذا بشكل خاص في مصر، حيث يوجد انسجام بين السياسات / الممارسات المحلية والسلوك في الجمعية العامة للأمم المتحدة، فيما يتعلق بالقضايا المتعلقة بالفضاء السيبراني. أمّا السلوكيات المحلية والدولية للمغرب والأردن فإنها أقل انسجاماً. فمن ناحية، يتولى البَلَدان مراقبة المحتوى على المستوى المحلي، من خلال مزيج من التدابير الرسمية وغير الرسمية. ومن ناحية أخرى، فإنهما يدعمان، على المستوى الدولي، عمليات كلٍّ من الولايات المتحدة الأمريكية وروسيا لوضع معايير سلوك الدولة في الفضاء السيبراني. ويمكن الافتراض بأنّ التناقض على المستويين المحلي والدولي يرجع إلى تفضيلهما عدم الانحياز إلى أي طرف في حلول حوكمة الإنترنت.

### مصر

استثمرت مصر في قطاع تكنولوجيا المعلومات والاتصالات لتعزيز التنمية الاقتصادية (Saleh, 2012). واختارت الحكومة نهجاً مركزيّاً (Wheeler, 2003)، وأصدرت

3) هذا الانقسام ليس واضحًا كوضوح حدود الدول الغربية. فعلى سبيل المثال، فإنّ "دعاة حماية البيانات الأوروبيين المتشددين الذين يرغبون في تحديد تدفقات المعلومات، والعديد من المحاربين الإلكترونيين في الجيش الأمريكي [...] جميعهم من أنصار الاتساق" (Mueller, 2017, p. 35).

استراتيجية وطنية للإنترنت خلال القمة الاقتصادية لمنطقة الشرق الأوسط وشمال أفريقيا عام 1994. وهدفت الخطة إلى الانتقال الاجتماعي والاقتصادي الذي تمحور حول فكرة الانتقال من الاعتماد على الصناعة إلى الاقتصاد القائم على المعرفة. وفي السنوات التالية، اتخذت الحكومة بقيادة الرئيس حسني مبارك سلسلة من المبادرات لنشر تكنولوجيا المعلومات والاتصالات بين السكان. أسفرت هذه الجهود عن نتائج ذات صلة، حيث ارتفع عدد مستخدمي الإنترنت في أقلّ من عقدين من 438,208 (2000) إلى 48 مليون (2019) وفقاً لإحصائيات موقع (www.internetlivestats.com) التي جمعها الاتحاد الدولي للاتصالات (ITU) والبنك الدولي وشعبة السكان في الأمم المتحدة، بنسبة انتشار بلغت 55,7٪ (Arab Republic of Egypt, 2020). وعلاوة على ذلك، يوجد أكثر من 200 مزوِّد معتمَد لخدمة الإنترنت (ISPs). ينعكس النموذج المركزي في سيطرة الحكومة على شؤون وسلطات تكنولوجيا المعلومات والاتصالات أيضاً؛ فعلى سبيل المثال، لا يتمتع الجهاز القومي لتنظيم الاتصالات (NTRA) الذي ينظم جميع أنشطة تكنولوجيا المعلومات والاتصالات ومزودي خدمة الإنترنت بالاستقلال الرسمي عن الحكومة (Article 19, 2015). وبشكل عام، تحتفظ الحكومة "بسيطرة كبيرة على البنية التحتية للإنترنت، وقد قامت بتقييد الاتصال" (Freedom House, 2019a).

ازداد التدخل الحكومي للتنظيم والسيطرة على المحتوى عبر الإنترنت على مر السنين. ففي المرحلة الأولى، قبل ثورة 2011، ذكر تقرير صادر عن مبادرة "الشبكة المفتوحة" (OpenNet) أنه "لا يوجد دليل على تصفية أو فلترة الإنترنت في مصر، على الرغم من حظر مجموعة صغيرة من المواقع الحسّاسة سياسيّاً في الماضي" (OpenNet Initiative, 2009). وفي خضم الثورة، في يناير 2011، تمكنت السلطات الوطنية من إغلاق الإنترنت في عدة مناسبات. وبعيداً عن الفترة السياسية القصيرة والفاصلة لمحمد مرسي، ومع ظهور عبد الفتاح السيسي، بدأت السلطات في الانخراط بشكل أكبر في مراقبة الإنترنت والرقابة التعسفية، وإغلاق المواقع الإلكترونية. يخضع فيسبوك (Facebook) على وجه الخصوص للتدقيق، ويُستهدَف بطلبات إغلاق صفحات معينة (Freedom House, 2020a). في عام 2018، قررت الحكومة إطلاق نسختها الخاصة من فيسبوك، دون جدوى، وهي منصة اجتماعية تسمى "وجه مصر" (Egypt Face).

وفيما يتعلق بالمواقف الدولية، تعد مصر لاعباً نشطاً للغاية، وتشارك في المبادرات العالمية الرئيسية، بما في ذلك تلك التي ترعاها دول الاتحاد الأوروبي والدول "ذات التفكير المماثل". وعلى سبيل المثال، كانت مصر وفرنسا المبادرتين باقتراح تم تقديمه إلى رئيس فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، لإنشاء برنامج عمل ترعاه الآن 47 دولة أخرى من الدول الأعضاء في الأمم المتحدة. تدعو المقترحات إلى اتخاذ خطوات ملموسة من أجل تحقيق نتائج عملية بشأن الأمن السيبراني الدولي. ومع ذلك، غالباً ما تعكس مواقف مصر في الأمم المتحدة مواقف الدول التي تتخذ نهج "الاتساق" (النموذج التوافقي)، مثل روسيا (Dominioni, 2020b). ويتضح هذا بشكل خاصّ في أنماط تصويت مصر في الأمم المتحدة على بعض القرارات الرئيسية، بما في ذلك إنشاء فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي، وفريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. أعربت مصر في هذه المنتديات عن رغبتها في "تفعيل القواعد والمعايير الحاليّة التي أقرتها الجمعية العامة للأمم المتحدة سابقاً من خلال تحسين وضعها، وجعلها أكثر إلزاماً لجميع الدول" (UN OEWG, 2020).

## الأردن

يسعى الأردن إلى تطوير تكنولوجيا المعلومات والاتصالات كوسيلة لتعزيز التنوع الاقتصادي وتحفيز النمو (Ein-Dor et al., 2005). وعلى وجه الخصوص، أعرب الملك عبد الله الثاني، منذ أوائل العقد الأول من القرن الحادي والعشرين، عن إيمانه الكامل ودعمه لنشر تكنولوجيا المعلومات والاتصالات في البلاد (Al-Jaghouob & Westrup, 2003). وأدّت المبادرات المتعددة التي اجتذبت مشاركة المانحين الدوليين من القطاعين العام والخاصّ (مثل البنك الدولي ومايكروسوفت) إلى نشر تقنيات جديدة بين السكان إلى جانب جهود التعليم (Al-Jaghouob & Westrup, 2003). وارتفعت نسبة مستخدمي الإنترنت بين السكان الأردنيين من 2,6٪ عام 2000 إلى 66,8٪ عام 2017 (World Bank, 2020). واختارت الحكومة الأردنية نهجاً بين القطاعين العام والخاص لتطوير تكنولوجيا المعلومات والاتصالات. وتمّ تحديد الاستراتيجية الرئيسية في مبادرة "وصول" (REACH) التي قدّمت نهجاً وطنيّاً وحدّدت خطة عمل واضحة للأردن لتطوير نموذج تنافسي لتكنولوجيا المعلومات والاتصالات، مثل ذلك المعتمد في إيرلندا وسنغافورة (Al-Jaghouob & Westrup, 2003). ومع ذلك، تحتفظ الدولة ببعض السيطرة على البنى التحتية للإنترنت (Freedom House, 2020b). ويوجد حاليّاً خمسة مزودي خدمة إنترنت رئيسيين في الأردن، وهم زين وأورانج وأمنية وتي إي داتا وداماماكس. وتنظم هيئة تنظيم الاتصالات (TRC) سوق خدمات الإنترنت، وهي هيئة مستقلة، ولكنّها تخضع للمساءلة أمام وزارة الاقتصاد الرقمي وريادة الأعمال (MoDEE).

تطورت سياسات الأردن المتعلقة بالتحكم في محتوى الإنترنت والرقابة عليه على مر السنين؛ فقد كانت السلطات حريصة على تجنب حجب الإنترنت خلال العقد الأول من القرن الحادي والعشرين، بما في ذلك حجب المنصات الاجتماعية مثل فيسبوك وتويتر ويوتيوب. وبالإضافة إلى ذلك، وفيما يتعلق بالرقابة أو تقييد المحتوى، بدت السلطات الأردنية في تلك السنوات غير متأكدة من حرية الإنترنت ومن أفضل طريقة لتنظيمها (Freedom House, 2011). وفي يناير 2010، تم فرض تحول كبير في حكم محكمة النقض الذي أكد أنّ المواقع الإلكترونية ووسائل الإعلام الإلكترونية يجب أن تمتثل لقانون الصحافة والمطبوعات (PPL) (Freedom House, 2011). وعلاوة على ذلك، أقرّ الأردن في السنوات التي أعقبت الربيع العربي العديد من القوانين التي فرضت قيوداً مرهقة على حرية الإنترنت، بما في ذلك تعديلات على قانون الصحافة والمطبوعات الذي أعلن أنّ أي موقع ويب أو منصة تنشر الأخبار يجب أن تسجل لدى الحكومة.

وعلى المستوى الدولي – وخاصة فيما يتعلق بتصويت الجمعية العامة للأمم المتحدة حول فريق الخبراء الحكوميين التابع للأمم المتحدة، المعني بتعزيز سلوك الدولة المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي، وفريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي – اتخذ الأردن نهجاً أكثر اعتدالاً من مصر، حيث رحّب بالمبادرات الروسية وبمبادرات الولايات المتحدة الأمريكية. ومع ذلك، التزم الأردن الصمت إلى حدّ ما في توضيح مواقفه، ففي الداخل يبدو أنه يحافظ على السيطرة على المعلومات، بينما كان أكثر حذراً على المستوى الدولي في اتخاذ موقف، وفي إعلان مواقفه بوضوح. ويتماشى هذا النهج مع كل من نهج ما يسمى ببلدان عدم الانحياز، ومع استراتيجية عمّان المقصودة التي "تسمح للأردن بأن يظهر [مع اهتمام خاص بالدول المانحة الغربية] كنظام سياسيّ حديث وتقدميّ نسبيّاً" (Yom, 2009, p. 152).

## المغرب

بدأ المغرب تحرير قطاع الاتصالات في أواخر التسعينيات؛ وتمت إدارة هذه العملية من قبل الوكالة الوطنية لتنظيم الاتصالات (ANRT). ومع ذلك، فإنّ البنية التحتية لتكنولوجيا المعلومات والاتصالات لا تزال بأكملها مملوكة للدولة. ويوجد في الوقت الحاضر ثلاثة مزودي خدمة إنترنت روّاد في المغرب: اتصالات المغرب، أورانج المغرب، وشركة إنوي. ولم تفرض الحكومة، على مر السنين، أية قيود على الاتصال، ولا تمارس أية سيطرة تقنية أو قانونية على البنية التحتية للإنترنت لهذا الغرض (Freedom House, 2019b).

إنّ الوصول إلى الإنترنت في المغرب مفتوح وغير مقيد في معظمه؛ وتدير الوكالة الوطنية لتنظيم الاتصالات أيضاً نطاق المستوى الأعلى للدولة (ma.) بطريقة غير تمييزية. ومع ذلك، فإنّ احتمالات السيطرة النظامية المحتملة على المحتوى عالية لأنّ العمود الفقري للإنترنت مركزي للغاية (Freedom House, 2019b). وفي هذا الصدد، فإنّ سياسات الرقابة والتصفية (الفلترة) المغربية جراحية للغاية ومُركّزة (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020). ويتم فرض هذه السياسات من خلال تقييد الوصول إلى مواقع ويب معينة، ومراقبة وسائل التواصل الاجتماعي، والحدّ من استخدام التورنت (مشاركة الملفات ونقلها مباشرة بين مستخدمي الإنترنت دون وجود وسيط) (Internet Censorship Map, 2017). وعلاوة على ذلك، تستهدف السلطات – عندما يتعين عليها التدخل – الأفراد بشكل مباشر عن طريق الاتصال بالمستخدِم وتطلب منه إزالة المحتوى (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020).

وفيما يتعلق بالمحتوى، تنشط السلطات بشكل خاص في كبح جميع المحتويات عبر الإنترنت التي تعتبر "ضارة بالإسلام أو النظام الملكي أو وحدة الأراضي أو النظام العام" (Reporters Without Borders, 2016). والقانون ضارّ بشكل خاص بالصحافة الاستقصائية، لكنّ آثاره امتدت إلى مجتمع الإنترنت ككلّ. ومع ذلك، أشارت منظمة فريدوم هاوس (Freedom House) إلى اتجاه إيجابي يتمثل في أنها لم تُبَلَّغ عن أيّ حظر للإنترنت من قبل الحكومة منذ عام 2013، ولم يتمّ إغلاق الإنترنت بشكل عام أو بشكل محلي حتى الآن.

على المستوى الدولي، يبدو أنّ المغرب يتبع نهج حركة عدم الانحياز (NAM) الذي يتضمن سياسة منفتحة تجاه أيّ نوع من المبادرات بغضّ النظر عن المبادر بها، بما في ذلك الوثائق الملزِمة، مثل اتفاقية بودابست بشأن الجرائم السيبرانية (تمّ التصديق عليها في 2018). وعلى وجه الخصوص، وكما ورد في *ورقة عمل حركة عدم الانحياز للدورة التخصصية الثانية لفريق الأمم المتحدة العامل المفتوح العضوية، والمعني بالتطورات في ميدان تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي*، وهي "تمثل العملية المُتَّفَق عليها بين الأطراف المتعددة، والقائمة على توافق الآراء داخل منظومة الأمم المتحدة، وأفضل طريقة لضمان أنّ الترتيبات في هذا المجال تعالج اهتمامات جميع الدول، ومن ثَمّ تكون منصفة وشاملة ومُنفَّذة بشكل فعال" (NAM, 2020).

## معالجة التضليل

أصدر المنتدى الاقتصادي العالمي عام 2013 تقريراً عن المخاطر العالمية لحملات التضليل الرقمي[4] الضخمة في خضم المخاطر التكنولوجية والجيوسياسية (Zollo, 2019). وأصبحت هذه الظاهرة أكثر إشكالية خلال جائحة كورونا. وقد اتخذت الجهات الفاعلة العامة، مثل الحكومات والمنظمات الدولية، والجهات الفاعلة الخاصة، والصحف ومنصات التواصل الاجتماعي، تدابير لمكافحة انتشار المعلومات المُضلِّلة عبر الإنترنت. ومع ذلك، يُفترَض أنه سيكون من الممكن – في بعض السياقات المحددة – استخدام السياسات العامة الهادفة إلى معالجة المعلومات المُضلِّلة لكبح حركات المعارضة ومجموعات المجتمع المدني وحرية الإنترنت ككلّ. وفي جميع البلدان التي هي موضوع الدراسة، توجد سوابق لمكافحة سياسات وممارسات المعلومات المُضلِّلة، تمّ تطويرها قبل تفشي جائحة كورونا. وفي الواقع، قامت دول مصر والمغرب والأردن بتجهيز نفسها بقوانين تهدف إلى مكافحة دعاية التطرف والمحتوى الإرهابي على الإنترنت. وقد لوحظت بالفعل انتهاكات لهذه القوانين في مناسبات متعددة[5]. ففيما يتعلق بمواجهة المعلومات المُضلِّلة المتعلقة بجائحة كورونا، استخدمت السلطات في بعض الحالات الأدوات القانونية الموجودة بالفعل، وطوّرت بلدان أخرى سياسات جديدة تماماً لاستهداف وباء المعلومات. ومع ذلك، فإنّ البحث الذي تم إجراؤه حتى الآن لم يذكر أيّ تعريف مُحدَّد أو تمييز لمصطلحات: المعلومات المُضلِّلَة / المعلومات الخاطئة / الأخبار المُزيَّفة التي تستخدمها السلطات في البلدان موضوع الدراسة.

تبحث الأقسام التالية في الأساليب المعتمدة في مصر والمغرب والأردن لمواجهة ممارسات التضليل الإعلامي. وتصور الحالات قيد الدراسة ثلاثَ سلوكيات مختلفة فيما يتعلق بتبني وسوء استخدام / استخدام سياسات المعلومات المُضلِّلة المضادة فيما يتعلق بجائحة كورونا. ففي مصر، حيث حرية الإنترنت محدودة للغاية (بنسبة 100/26) (Freedom House, 2020a)، لم تكن السلطات بحاجة إلى اعتماد المزيد من القيود المُحدِّدة لحرية الإنترنت لمعالجة المعلومات المُضلِّلة. ففي هذه الحالة، كانت السلطات تستخدم القوانين الحالية للحدّ من أي روايات بديلة مُحتمَلة حول إدارة الجائحة، ولا سيّما تلك الواردة من مصادر موثوقة (مثل الأطباء والطاقم الطبي). وفي المغرب، حيث يتمّ التسامح مع حرية الإنترنت بدرجة أكبر (100/52) (Freedom house, 2020c)، حاول النظام تمرير قانون جديد أكثر تقييداً ضدّ التحكم في المحتوى عبر الإنترنت، ولكنّه تعرض لانتقاد شديد من قبل المجتمع المدني النشط، وتمّ بالتالي تعليقه. ويتمتع الأردن بمستوى مماثل من حرية الإنترنت (100/49) (Freedom house, 2020b)، إلّا أنّ السلطات، على الرغم من وجود إطار قانوني بالفعل ضدّ التضليل الإعلامي، قرّرت تنفيذ سياسات أكثر صرامة لمحاربة هذه الظاهرة، ولجأت إلى إساءة استخدامها مثل كبح المعارضة السياسية، كما حدث مع "احتجاجات المعلمين".

إنّ هذه السلوكيات الثلاثة المختلفة هي أيضاً رمزية من حيث حالة النظام، أو القوة التنظيمية، في كل بلد قيد الدراسة. المغرب نظام هجين مستقر وجد توازناً مستداماً

4) يتمّ في هذا الفصل استخدام المعلومات المُضلِّلَة كمفهوم شامل يتضمن المعلومات الخاطئة والأخبار المزيّفة وأنماط اضطراب المعلومات الأخرى ذات الصلة.

5) انظر، على سبيل المثال، *تقرير يوروميد رايتس* (EuroMed Rights) المتاح على: https://euromedrights.org/wp-content/uploads/2018/03/EuroMed-Rights-Report-on-Counter-terrorism-and-Human-Rights.pdf

تعتبر السلطات الأردنية الإنترنت مصدر عدم استقرار في النظام

بين الحكام والمحكومين منذ الإصلاحات الدستورية المهمة في 2011. كان من الممكن أن يتسبب القانون 22,20 في اختلال التوازن، ولذلك تمّ تعليقه. وتشير الأدلة المُتناقَلة إلى أنّ النظام لا يعتبر حرية الإنترنت تهديداً لاستقراره (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020). أمّا مصر فتملك نظاماً استبداديّاً مستقراً، ومنذ أعقاب ثورة الربيع العربي، ولا سيّما منذ بدء حكم إدارة السيسي، نفَّذ النظام سياسات مهمة للحدّ من حرية الإنترنت، تجعل الآن ثورة أخرى قائمة على الإنترنت مستحيلة عمليّاً (Researcher, AFTEEGYPT, personal communication, November 10, 2020; J. Shea, TIMEP, personal communication, November 11, 2020). وفي ضوء هذه الخلفية، كان النظام مجهزاً جيداً للحدّ من المعلومات المُضلِّلة المتعلقة بجائحة كورونا. والأردن أيضاً نظام استبدادي، لكنّه يُعتبر قوة تنظيمية أقلّ استقراراً. وفي واقع الأمر، فقد الناس الثقة بالمؤسسات العامة (IRI, 2018). وقد كانت هذه عملية طويلة من خيبات الأمل بدأت منذ منتصف التسعينيات (M. Torki, Yarmouk University, personal communication, October 30, 2020). وفي هذا السياق، تعتبر السلطات الأردنية الإنترنت مصدر عدم استقرار في النظام (M. Torki, Yarmouk University, personal communication, October 30, 2020; R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). لذلك، وكما يتضح من التحليل أعلاه، هناك حالات ملحوظة لسوء استخدام السياسات العامة لمعالجة المعلومات المُضلِّلة حول جائحة كورونا. فقد يكون التأثير العام على حرية الإنترنت أمراً مهمّاً للدولة.

## مصر

ضرب وباء المعلومات مصر في بداية جائحة كورونا. ففي مارس 2020 كانت هناك ثلاثة بيانات رئيسية، من رئيس الوزراء والنائب العام ورئيس المجلس الأعلى للإعلام، تهدف إلى منع السكان من مشاركة معلومات مُضلِّلة حول جائحة كورونا. وكانت منصات التواصل الاجتماعي من بين مصادر القلق الرئيسية (Researcher, AFTEEGYPT, personal communication, November 9, 2020)، إذ يستخدمها المصريون على نطاق واسع، لأنّ أنواعاً أخرى من وسائل الإعلام تخضع بالفعل لسيطرة الدولة الكاملة. ولم تقم السلطات بتمرير قوانين أو لوائح معينة للحدّ من المعلومات المُضلِّلة، بل اعتمدت على القوانين الموجودة سابقاً مثل القانون رقم 175 لسنة 2018 بشأن مكافحة الجرائم السيبرانية، والقانون رقم 180 لسنة 2018 بشأن تنظيم الصحافة والإعلام، والقانون رقم 58 لسنة 1937 وتعديلاته على قانون العقوبات. وتمنح هذه القوانين السلطات صلاحيات كافية للتدخل ضدّ أي منشورات أو صحف أو وسائل إعلامية أو مواد إعلانية تحتوي على معلومات يُعتقَد أنها تهدد الأمن القومي؛ أو تعكّر صفو السلم العام؛ أو تروج للتمييز أو العنف أو العنصرية أو الكراهية أو عدم التسامح (Law 180, art. 4, 2018). وفي مثل هذه الحالات، يمنح القانون 180 المجلس الأعلى للإعلام سلطة حظر أو تعليق توزيع أو بثّ أو تشغيل أيٍّ من وسائل الإعلام، أو تعليق أو حظر أيّ موقع شخصي أو مدونة أو حساب على وسائل التواصل الاجتماعي لديه أكثر من 5000 متابع.

تحولت السلطات، بعد فترة أولى من المبادرات الإيجابية، مثل فضح جهود الأخبار الكاذبة المتعلقة بجائحة كورونا التي قام بها المركز الإعلامي لمجلس الوزراء المصري (مؤسسة عامة)، إلى حملة أكثر انتشاراً لكبح أيّ نوع من المعارضة، وإسكات الانتقادات لكيفية تعامل الحكومة المصرية مع الجائحة (AFTEEGYPT, 2020). وفي واقع الأمر، لم ترغب الحكومة في انتشار روايات بديلة لروايتها الرسمية (J. Shea, TIMEP, personal

communication, November 11, 2020)، فحدث تدقيق على الأطباء والممرضات والموظفين الطبيين الآخرين بشكل خاص من قبل السلطات التي لجأت إلى التحكم بنشاطهم عبر الإنترنت. وقد تمّ بين أبريل ويونيو 2020، اعتقال ستة أطباء بتهمة التعبير عن آرائهم على وسائل التواصل الاجتماعي (AFTEEGYPT, 2020). ووفقاً للتقرير *ربع السنوي عن حالة حرية التعبير في مصر*، ارتفع معدل انتهاك الحقّ في حرية التعبير على الإنترنت بين أبريل ويونيو 2020 بنسبة 500٪ (AFTEEGYPT, 2020).

## الأردن

مع تفشي الجائحة في البلاد، أصدر الملك عبد الله الثاني في منتصف مارس 2020 مرسوماً ملكيّاً سمح للحكومة باتخاذ إجراءات استثنائية. وكان أحدها أمر الدفاع رقم 8 الصادر في 15 أبريل 2020 الذي يحظر "نشر أو إعادة نشر أو تداول أي خبر عن الجائحة بغرض ترويع الناس أو إثارة الذعر بينهم عبر وسائل الإعلام أو الاتصالات أو وسائل التواصل الاجتماعي". وقد يتعرض المخالفون لخطر السجن لمدة تصل إلى ثلاث سنوات. ولم تكن الدولة جديدة على هذا النوع من القيود فيما يتعلق بحرية التعبير، فهناك قوانين أخرى تُجرِّم الانتقادات المُوجَّهة للملك والعائلة المالكة والمؤسسات العامة الأخرى (M. Torki, Yarmouk University, personal communication, October 30, 2020). وعلاوة على ذلك، وافق البرلمان في فبراير 2019 على قانون مُعدَّل للجرائم السيبرانية تضمن تعريفًا غامضاً لـ "خطاب الكراهية" على أنه "كلّ كتابة وكلّ خطاب أو عمل يهدف إلى إثارة الفتنة الطائفية أو العرقية، أو الدعوة إلى العنف، أو إثارة الصراع بين أتباع الديانات المختلفة أو مختلف مكونات الأمة" (Accessnow, 2019). وبالمثل، فإنّ نصّ أمر الدفاع رقم 8 غامض بشأن ما يُعتبَر معلومات مُضلِّلة (R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). وعلى الرغم من أنّ رئيس الوزراء عمر الرزاز أكّد أنّ القانون سيتم تطبيقه "على أضيق نطاق" (Freedom House, 2020b)، فقد كانت هناك عدة قضايا متنازع عليها فيما يتعلق بتطبيقه حتى قبل دخوله حيز التنفيذ (HRW, 2020a).

ومنذ بداية الجائحة، كان هناك العديد من الدعاوى القضائية ضد أفراد شاركوا أو نشروا شيئاً ما على وسائل التواصل الاجتماعي، وقد بدأت تلك الدعاوى على أساس قانون الجرائم السيبرانية أو أمر الدفاع رقم 8. ومن بين الأحداث التي لاحظتها منظمات حقوق الإنسان، قمع المنشورات عبر الإنترنت التي تتعلق بما يسمى "احتجاج المعلمين" الذي حدث في صيف 2020 (HRW, 2020b)، إلا أنه لم يتم رصد أي حالات إدانة بنفس التهم (Q. Suwan, Jordan Open Source, personal communication, November 9, 2020). ويمكن القول إنها "ورقة" إضافية يمكن للنظام أن يلعبها لردع المزيد من السخط (R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). يتم تحديد هوية المستخدمين من خلال نظام فعّال للمراقبة، ويعتمد على آليات بسيطة، مثل مراقبة منشورات وسائل التواصل الاجتماعي العامة (R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). وبمجرد تحديد المستخدم، يكون لدى السلطات عدة طرق للتدخل: فهي تتواصل مباشرة مع مؤلف المنشور، وتطلب منه إغلاقه، أو الشروع في مقاضاته، أو تحضر السلطات مباشرة إلى منزل المؤلف وتأخذه من هناك، وتكون أحياناً بملابس مدنية (M. Torki, Yarmouk University, personal communication, October 30, 2020; R. Sharbain, Jordan Open Source, personal communication, November 9, 2020).

## المغرب

إن الجمع بين الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات ومستوى الأمية المرتفع هو عامل جذب للمعلومات المُضلِّلة، وهي مشكلة مستوطنة وطويلة الأمد تؤثر على البلاد. ومع ذلك، لم يكن لدى السلطة المغربية سياسة خاصة بوسائل التواصل الاجتماعي حتى بداية الجائحة. لم يُستخدَم قانون مكافحة الإرهاب الذي تم تبنّيه في عام 2003 للحدّ من وسائل الإعلام منذ 2013، عندما حجبت السلطات المغربية المواقع الإلكترونية للمَنفَذ الإخباري الاستقصائي لكومي بزعم التغاضي عن الإرهاب (Freedom House, 2020c). وفي منتصف شهر مارس، أصدرت الحكومة القانون رقم 22,20 الذي سرعان ما أطلق عليه اسم "*لا لوا بافيت*[6]" (la loi bavette)؛ ووفقاً لهذا النص القانوني الجديد، "يُعاقَب كلّ من يستخدم شبكات التواصل الاجتماعي، أو شبكات البث المفتوحة، أو الشبكات المماثلة، عن عمد لنشر أو ترويج محتوى إلكتروني يحتوي على معلومات كاذبة، بالحبس من ثلاثة أشهر إلى سنتين، وبغرامة تتراوح بين 1000 و 5000 درهم [105 دولارات إلى 525 دولاراً]، أو أيٍّ من هاتين العقوبتين فقط" (Law 22.20, Article 16, 2020). صدم هذا القانون الجديد الشعب المغربي لأنه حتى تلك اللحظة كان المغرب يتمتع بسياسة إيجابية نسبية لحرية التعبير على الإنترنت (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020). وردّاً على ذلك، اعترضت العديد من منظمات المجتمع المدني (CSOs) بشدة على القانون، وحققت بعض النجاح، إذ تمّ تعليقه في مايو 2020 حتى انتهاء الأزمة الصحية. وعلى الرغم من تعليق القانون، فإنّ السلطات المغربية لديها أدوات أخرى لمعالجة التضليل، مثل قانون العقوبات، وقانون مكافحة الإرهاب، وقانون الصحافة.

وفي ضوء هذا الإطار القانوني، تمّ في الأشهر التي أعقبت تفشي الجائحة اعتقال العديد من الأشخاص لمشاركتهم أخباراً كاذبة على منصات التواصل الاجتماعي. كانت المعتَقَلة الأولى "مي نعيمة"، مشهورة نسبيّاً وذات تأثير محلّي، وقد ادّعت، في مقطع فيديو نُشر على يوتيوب، أنّ جائحة كورونا غير موجودة. وتبع ذلك حالات أخرى، وتمّ اعتقال ما لا يقلّ عن 12 شخصاً بنفس التهم (Mebtoul, 2020). وتراقب المديرية العامة للأمن القومي منصات وسائل التواصل الاجتماعي عن كثب، لمكافحة حوادث التضليل فيما يخص جائحة كورونا، ولديها برامج مراقبة متطورة للغاية (Freedom House, 2020c). وتفضل السلطات عدم إغلاق الصفحات أو طلب حظر منشور، ولكنها تفضل مخاطبة المستخدمين مباشرة، ولم ترد تقارير عن إساءة استخدام سياسات مكافحة التضليل لاستهداف الأشخاص لأسباب أخرى غير نشر أخبار كاذبة حول الجائحة (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020).

6) قانون التكميم (ترجمة المؤلف)

## دعم الاتحاد الأوروبي لمواجهة المعلومات المُضلِّلة في منطقة الشرق الأوسط وشمال أفريقيا

لقد تطور نهج الاتحاد الأوروبي في التعامل مع المعلومات المُضلِّلة في السنوات الخمس الماضية من نهج يركز بشكل خاص على حملات التضليل الموجهة – مثل حملات التضليل المستوحاة من الكرملين (التي تناولتها فرقة عمل إيست ستراتكوم (East StratCom التابعة لخدمة العمل الخارجي الأوروبي [ESCTF]) أو التركيز على مواجهة ظاهرة التطرف في العالم العربي، وخاصة لمواجهة رواية تنظيم داعش (التي تناولها المنتدى الأوروبي لمكافحة الإرهاب) – إلى سياسات أكثر تطلعًا إلى الداخل، بعد التدخل في الانتخابات الرئاسية للولايات المتحدة في عام 2016. وتمثل الجهود المحلية لتعزيز مناعة الاتحاد الأوروبي ضد المعلومات المُضلِّلة جانباً مهمّاً أيضاً من مشاركة الاتحاد الأوروبي في مكافحة المعلومات المُضلِّلة، لأنها يمكن أن تكون مصدر إلهام لإيجاد الحلول المؤسساتية والتنظيمية، بما في ذلك قانون الممارسات بشأن المعلومات المُضلِّلة (EC, 2018a)، وخطة العمل ضدّ المعلومات المُضلِّلة (ديسمبر 2018)، ونظام التنبيه السريع (مارس 2019)، وخطة العمل الأوروبية للديمقراطية (2020)، وقوانين السوق الرقمية (DMA)، وقانون الخدمة الرقمية (DSA, 2020).

لقد تطور نهج الاتحاد الأوروبي في التعامل مع المعلومات المُضلِّلة في السنوات الخمس الماضية من نهج يركز بشكل خاص على حملات التضليل الموجهة إلى سياسات أكثر تطلعًا إلى الداخل

وفي ضوء التزام الاتحاد الأوروبي بإنترنت مفتوح وعالمي ويتمتع بالمناعة في جميع أنحاء العالم (EC, 2020)، يشكل بناء القدرات الإلكترونية لبنة أساسية في الدبلوماسية السيبرانية للاتحاد الأوروبي، بما في ذلك برامج التعاون الإنمائي لتعزيز وحماية حقوق الإنسان، والمساواة الرقمية بين الجنسين، وسيادة القانون والأمن. وانعكست المبادئ التوجيهية الرئيسية في اختتام اجتماع مجلس الاتحاد الأوروبي في يونيو 2018، إذ تدمج هذه الوثيقة وتُتمِّم الدروس الداخلية، وأفضل الممارسات من الدول الأعضاء، والمبادرات المختلفة المتخذة على مستوى الاتحاد الأوروبي. ويرحب مجلس الاتحاد الأوروبي في استنتاجاته أيضاً بوضع "المبادئ التوجيهية التشغيلية" من قبل مفوضية الاتحاد الأوروبي لبناء القدرات الإلكترونية في البلدان الثالثة (Council of the EU, 2018). ويبحث الاتحاد الأوروبي بنشاط عن تنسيق أكبر على المستوى الدولي لتعزيز نهج منسّق للأمن السيبراني والمناعة السيبرانية. وبهذا المعنى، يلعب بناء القدرات الإلكترونية دوراً رئيسيّاً في تعزيز التعاون مع البلدان الأخرى.

لقد قام الاتحاد الأوروبي حتى الآن بتمويل 37 مشروعاً في جميع أنحاء العالم تتعلق ببناء القدرات الإلكترونية (Cybil Portal, n.d.). وعلى سبيل المثال، فيما يتعلق بالدول قيد الدراسة، شارك الاتحاد الأوروبي في تمويل مشروع سايبر ساوث مع مجلس أوروبا (CoE, n.d.). ويهدف هذا المشروع إلى تعزيز القدرات التشريعية والمؤسساتية بشأن الجرائم السيبرانية والاعتداءات الإلكترونية الأخرى، بما يتماشى مع متطلبات حقوق الإنسان وسيادة القانون في الجزائر والأردن ولبنان والمغرب وتونس. ومع ذلك، يمكن معالجة المعلومات المُضلِّلة من خلال مبادرات أخرى. ومن وجهة نظر سياسة الجوار الأوروبية، يشارك الاتحاد الأوروبي بنشاط في العديد من المشاريع المختلفة التي تضم جهات فاعلة أساسية لمواجهة المعلومات المُضلِّلة والأخبار المُزيَّفة. ويهدف بعضها إلى دعم وسائل الإعلام في المنطقة، مثل "تطوير الصحافة الأوروبية القائمة على المعرفة والمتعلقة بجيران أوروبا" (2018-2019)، و "ساوثميد ويا" (SouthMed WiA) (2017-2019)، و "أوبن ميديا هاب" (2016-2019) (Open Media Hub). وتهدف المشاريع الأخرى إلى تعزيز المهارات الرقمية للشباب وتعزيز الوعي، مثل "جينيريشن وات؟ عربي" (2017-2018) (Generation What? Arabic) و "د-جيل" (D-Jil)

(2018-2022) و "نيت-ميد يوث" (2014-2018) (NET-MED Youth). ومع ذلك، لم يعثر هذا التحليل على أدلة تجريبية حول المشاريع أو البرامج التي موّلها الاتحاد الأوروبي سابقاً أو حاليّاً، والتي تهدف بشكل مباشر إلى مشاركة أفضل الممارسات أو الإرشادات، أو المساعدة لمعالجة المعلومات المُضلِّلة في منطقة الشرق الأوسط وشمال أفريقيا. ويمكن القول إنّ الافتقار إلى المشاريع المباشرة لمواجهة التضليل الإعلامي (ما بعد التطرف) في المنطقة تمّ تحديده من خلال عاملين رئيسيين: أولاً، طوّر الاتحاد الأوروبي مؤخراً فقط مجموعة محدَّدة ومنظَّمة من السياسات والإرشادات لمعالجة ظواهر مثل المعلومات المُضلِّلة والأخبار المُزيَّفة بطريقة منهجية ومنظمة. ثانياً، تصاعدت قضية التضليل في جدول الأعمال السياسي لبروكسل في السنوات القليلة الماضية. وفي هذا الصدد، كان موضوع المعلومات المُضلِّلة غائباً عن الأجندة الأوروبية للمفوضية حول الأمن 2015–2020، في حين يظهر باعتباره تهديداً أمنيّاً في *الاستراتيجية الأمنية الجديدة للاتحاد الأوروبي 2020-2025*.

## الاستنتاجات والتوصيات

درس هذا الفصل الكيفية التي يمكن فيها لحوكمة الإنترنت – ولا سيما السياسات العامة التي تعالج المعلومات المُضلِّلة أثناء جائحة كورونا – أن تلعب دوراً في تعزيز النظام غير الديمقراطي. وجاءت نتائج الدراسة ذات شقين: أولاً، يبدو أنّ البلدان التي تمت دراستها في هذا الفصل تفضّل نهج إدارة الإنترنت بالنهج الذي يشبه نموذج "الاتساق" (التوافقي) الذي يولي اهتماماً كبيراً لمراقبة المحتوى والرقابة. وثانياً، كشف التحليل أنّ ردود أفعال الأنظمة على المعلومات المُضلِّلة بشأن جائحة كورونا تمت معايرتها وفقاً لقدرتها التنظيمية (تماسك الدولة أو الجهاز الحاكم) وللتهديد المُتصوَّر الذي يمكن أن تشكله حرية التعبير على الإنترنت للنظام. تفسر هذه الحُجّة الثانية الفروق الدقيقة بين البلدان قيد الدراسة التي تتبنى جميعها نهج "الاتساق". ففي المغرب، تم تعليق القانون المطعون فيه رقم 22.20، ولكن يمكن إعادة تفعيله بمجرد انتهاء حالة الطوارئ الصحية. وفي مصر، تم تطبيق القوانين الموجودة مسبقاً مع التركيز بشكل خاص على العاملين في المجال الطبي، بما في ذلك الأطباء والممرضات. وفي الأردن، تم تطبيق أمر الدفاع الجديد رقم 8 بشكل عشوائي أيضاً لأغراض أخرى غير محاربة المعلومات المُضلِّلة المتعلقة بفيروس كورونا.

وفي هذا السياق، فإننا لا نجد الاتحاد الأوروبي يتخذ أيّ إجراء. ومع ذلك، قامت بروكسل خلال السنوات القليلة الماضية بتجهيز نفسها بسياسات مهمة للغاية، أثبتت فعاليتها في مواجهة حملات التضليل في الفترة التي سبقت انتخابات البرلمان الأوروبي في عام 2019، وأثبتت أنها كافية لمعالجة وباء المعلومات حول جائحة كورونا. وفي الوقت نفسه، قام الاتحاد الأوروبي بإدراجها في برامج الأمن السيبراني وبناء القدرات الإلكترونية الخاصة بسياسة الجوار الأوروبية الخاصة به. ومع ذلك، ظلّ التعاون الرسمي مع منطقة الشرق الأوسط وشمال أفريقيا، فيما يتعلق بموضوع المعلومات المُضلِّلة والأخبار المُزيَّفة والاضطرابات المعلوماتية الأخرى – حتى الآن – محدوداً للغاية وغير مباشر. وكما ذكرنا سابقاً، يمكن أن يكون عدم اتخاذ الإجراءات هذا مرتبطاً بسببين: أولاً، لأنّ الاتحاد الأوروبي كان يجهز نفسه بالاستراتيجية والأدوات الصحيحة لمواجهة هذه التحديات الجديدة. ثانياً، لم يتم التعرف رسميّاً على التهديدات المُتصوَّرة لهذه الظواهر رسميّاً إلا مؤخراً من خلال *الاستراتيجية الأمنية الجديدة للاتحاد الأوروبي 2020–2025*.

ومع ذلك، وبسبب الأهمية المتزايدة، وتزايد التهديدات من الفضاء الإلكتروني في الوقت نفسه، فإن التوصل إلى اتفاق على المستوى الدولي أمر أساسي. وفي هذا الصدد، يتعين على الاتحاد الأوروبي والجهات الفاعلة الدولية الأخرى أيضاً تعزيز جهودها لبناء المبادئ والمعايير والمبادئ التوجيهية لإدارة الإنترنت على المستوى المحلي. وبخلاف ذلك، وكما هو الحال في الوقت الراهن، يمكن لكلّ دولة صياغة سياساتها الرقمية الخاصة، بما في ذلك تلك التي تنتهك حقوق الإنسان. وفي الواقع، يمكن أن تتنكر سياسات التحكم في المحتوى في شكل سياسات ضد الأخبار المُزيَّفة أو المعلومات المُضلِّلة أو غيرها من التهديدات عبر الإنترنت بما في ذلك التطرف، إذ يمكن، من الناحية العملية، استخدامها لكبح حركات المعارضة أو مجموعات المجتمع المدني.

يمكن أن يلعب الاتحاد الأوروبي دوراً مهماً في هذا السياق لأنه حدد برامج مفصلة لمعالجة المعلومات المُضلِّلة، كانت ناجحة ومنسجمة مع مبادئ حرية الإنترنت وحقوق الإنسان. وفي ضوء ذلك، من المهم بالنسبة للإجراءات المستقبلية للاتحاد الأوروبي النظر في التوصيات التالية:

1. **يجب على الاتحاد الأوروبي تحديد نوع المناعة التي سيعززها في هذه البلدان، حيث توجد مقايضة محتملة بين مناعة النظام والمناعة المجتمعية.** وبالنظر إلى نموذج "الاتساق" (التوافقي) الذي تتبعه هذه البلدان (بدرجات مختلفة) لحوكمة الفضاء السيبراني، فإنّ قدرة الدولة على معالجة المعلومات المُضلِّلة تعتمد على السياسات والممارسات التي تتعارض مع مبدأ حرية الإنترنت. فعلى سبيل المثال، يوصَى بدعم إنشاء شبكة من الخبراء (مدققي الحقائق) الذين يمكنهم العمل ضد المعلومات المُضلِّلة في البلدان المختارة. قد يكون النموذج المقتَرَح لهذا هو مشروع "المرصد الاجتماعي للمعلومات المُضلِّلة وتحليل وسائل التواصل الاجتماعي (SOMA)". وعلاوة على ذلك، يعمل الاتحاد الأوروبي على إطلاق "المرصد الأوروبي للوسائط الرقمية (EDMO)" مع التركيز على أربعة مجالات رئيسية للتدخل: التحقق من الحقائق، والبحث، والتثقيف الإعلامي، وبحوث السياسات العامة، والتحليل. والفكرة الشاملة هي إنشاء مراصد وطنية متعددة في الدول الأعضاء في الاتحاد الأوروبي للعمل بانسجام ضد المعلومات المُضلِّلة. ويمكن أن يساعد إنشاء هياكل مماثلة في منطقة الشرق الأوسط وشمال أفريقيا في مواجهة الاضطرابات المعلوماتية.

2. **يجب على الاتحاد الأوروبي توخي الحذر لتجنب استخدام مشاريع بناء القدرات الإلكترونية لزيادة المراقبة والرقابة وغيرها من قدرات التحكم في المعلومات.** وتبدو إمكانية هذا الاحتمال أعلى في البلدان التي تعتبر فيها الإنترنت مصدراً لعدم الاستقرار. ولذلك، يجب على الاتحاد الأوروبي عند اقتراح وتنفيذ الإجراءات والمشاريع، النظر في القضية المتشعِبة من النهج القائم على حقوق الإنسان إلى بناء القدرات الإلكترونية (EC, 2020b). وبالإضافة إلى ذلك، من المهم أن يراقب الاتحاد الأوروبي المبادرات الأخرى (القانونية والتقنية وغير الرسمية) التي تتخذها الحكومة المستفيدة، والتي قد تتعارض مع قيم أو مصالح الاتحاد الأوروبي.

3. **يُعَدّ التعاون بين الحكومات أمراً مهماً، ولكن يتعين على الاتحاد الأوروبي أيضاً النظر في مشاركة جهات فاعلة أخرى غير حكومية، بما يتماشى مع نهج أصحاب الشأن المتعددين في الفضاء الإلكتروني.** ويجب أن تشمل هذه الجهات: منظمات المجتمع المدني التي تعمل كهيئات مراقبة، ومنصات وسائل التواصل الاجتماعي،

مثل فيسبوك أو تويتر، لتوسيع نطاق مشاركتها في الحدّ من المعلومات المُضلِّلة في بلدان ثالثة؛ والجهات المانحة والمنظمات الدولية الأخرى (مثل الاتحاد الدولي للاتصالات، ومنظمة الأمن والتعاون في أوروبا [OSCE]، ومنظمة حلف شمال الأطلسي [NATO]) التي تعمل على القضايا المتعلقة بالإنترنت.

4. **من منظور أوسع، قد يكون من المفيد تعزيز التعاون في مجال الأمن السيبراني وأمن المعلومات مع تلك البلدان التي لا تزال مترددة بشأن أفضلياتها السياسية فيما يتعلق بمعايير الفضاء السيبراني الدولية،** أو تلك التي تعتبر نفسها جزءاً من حركة عدم الانحياز. من خلال بناء تعاون أوثق، وعلى سبيل المثال يمكن للاتحاد الأوروبي – من خلال تضمين المزيد من الإشارات إلى القضايا المتعلقة بالإنترنت والمعلومات في أولويات شراكة سياسة الجوار الأوروبية – تحقيق ما يسمى "التشابك" (Nye, 2017)، ممّا قد يؤدي إلى ممارسة طرق إقناع أقوى للحصول على رؤى بديلة حول الموضوعات الرقمية، بما في ذلك المعلومات المُضلِّلة.

# المصادر والمراجع

ACCESSNOW. (2019). Cybercrime law in Jordan: pushing back on new amendments that could harm free expression and violate privacy. Retrieved from https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/

AL-JAGHOUOB, S., & WESTRUP, C. (2003). Jordan and ICT-led development: towards a competition state? Information, Technology & People, 16(1), 93-110.

ARAB REPUBLIC OF EGYPT. (2020). ICT indicators in brief . Ministry of Communication and Information Technology. Retrieved from http://www.mcit.gov.eg /Upcont/ Documents/Publications_19102020000_ICT _Indicators_in_Brief_ July_2020_EN.pdf

ARTICLE 19. (2015, April). Egypt: Telecommunication Regulation Law. Retrieved from https://www.article19.org/data/files/medialibrary/37966/Egypt-telecoms-report—-English.pdf )

ASSOCIATION FOR FREEDOM OF THOUGHT AND EXPRESSION IN EGYPT (AFTEEGYPT). (2020). Information blockade in the time of social distancing. Quarterly Report on the state of freedom of expression in Egypt second quarter. Retrieved from https://afteegypt.org/en/breaking_news-2/2020/10/07/20093-afteegypt.html

BANK, A., & EDEL, M. (2015). Authoritarian regime learning: comparative insights from the Arab uprisings (GIGA Working Paper 274). GIGA.

BARTLETT, J. (2018). The people vs. tech: how the Internet is killing democracy (and how we save it). New York: Penguin Random House.

BROEDERS, D. (2019). Mutually assured diplomacy: governance, 'unpeace' and diplomacy in cyberspace. Observer Research Foundation. Retrieved from https://www.orfonline.org/expert-speak/mutually-assured-diplomacy-governance-unpeace-diplomacy-cyberspace-56800/

BROEDERS, D., & CRISTIANO, F. (2020). Cyber norms and the United Nations: between strategic ambiguity and rules of the road. In S. Dominioni & F. Rugge (Eds.), Fragmenting the Internet: states' policies in the digital arena. ISPI Dossier. Retrieved from https://www.ispionline.it/it/pubblicazione/fragmenting-internet-states-policies-digital-arena-25416

BUNCE, V., & WOLCHIK, S. (2011). Defeating authoritarian leaders in post-communist countries. Cambridge: Cambridge University Press.

COUNCIL OF EUROPE (COE). (n.d.). CyberSouth activities. Retrieved from https://www.coe.int/en/web/cybercrime/cybersouth-activities

COUNCIL OF THE EUROPEAN UNION (COUNCIL OF THE EU). (2018). EU external cyber capacity building guidelines - Council conclusions. Retrieved from https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

CYBIL PORTAL. (n.d.). The knowledge portal for cyber capacity building. Retrieved February 15, 2021, from www.Cybilportal.org

DE LA CHAPELLE, B., & FEHLINGER, P. (2016). Jurisdiction on the Internet: from legal arms race to transnational cooperation (Paper Series 28). Centre for International Governance Innovation and Chatham House.

DEIBERT, J. (2019). The road to digital unfreedom: three painful truths about social media. Journal of Democracy, 30(1), 25-39.

DEIBERT, J., PALFREY, J., ROHOZINSKI, R., & ZITTRAIN, J. (Eds.). (2010). Access controlled. The shaping of power, rights, and rule in cyberspace. Cambridge: The MIT Press.

DEIBERT, J., PALFREY, J., ROHOZINSKI, R., & ZITTRAIN, J. (Eds.). (2008). Access denied: the practice and policy of global Internet filtering. Cambridge: The MIT Press.

DOMINIONI, S. (2020a). Panopticon 2.0? Why and how authoritarian regimes use AI surveillance. In F. Rugge (Ed.), AI in the age of cyber disorder (pp. 65-85). Milan: ISPI-Brookings.

DOMINIONI, S. (2020b). Does a North African Internet governance model exist? Evidence from Egypt and Morocco. In V. Talbot (Ed.), MED Report 2020 (pp. 102-105). Milan: ISPI.

DOMINIONI, S., & RUGGE F. (Eds.) (2020). Fragmenting the Internet: states' policies in the digital arena. ISPI Dossier. Retrieved from https://www.ispionline.it/it /pubblicazione/fragmenting-internet-states-policies-digital-arena-25416

EIN-DOR, P., GOODMAN, S., & WOLCOTT, P. (2005). The global diffusion of the Internet project: The Hashemite Kingdom of Jordan. The MOSAIC Group. Retrieved from http://mosaic.unomaha.edu/Jordan_1999.pdf

ELTANTAWY, N., & WIEST, J. B. (2011). Social media in the Egyptian revolution: reconsidering resource mobilization theory. International Journal of Communication, 5, 1207-24.

EUROPEAN COMMISSION (EC). (2018a). Code of practice on disinformation. Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

EUROPEAN COMMISSION (EC). (2020). The EU's cybersecurity strategy in the digital decade. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

FLORIDI, L. (2012). Hyperhistory and the philosophy of information policies. Philosophy & Technology, 25, 129-31.

FREEDOM HOUSE. (2011). Freedom on the Net – Jordan. Retrieved from https://www.refworld.org/docid/4dad51b627.html

FREEDOM HOUSE. (2019a). Freedom on the Net – Egypt. Retrieved from https://freedomhouse.org/country/egypt/freedom-net/2019

FREEDOM HOUSE. (2019b). Freedom on the Net – Morocco. Retrieved from https://freedomhouse.org/country/morocco/freedom-net/2019

FREEDOM HOUSE. (2020a). Freedom on the Net – Egypt. Retrieved from https://freedomhouse.org/country/egypt/freedom-net/2020

FREEDOM HOUSE. (2020b). Freedom on the Net – Jordan. Retrieved from https://freedomhouse.org/country/jordan/freedom-net/2020

FREEDOM HOUSE. (2020c). Freedom on the Net – Morocco. Retrieved from https://freedomhouse.org/country/morocco/freedom-net/2020

HUMAN RIGHTS WATCH (HRW). (2020a). Jordan: free speech threats under Covid-19 response. Retrieved from https://www.hrw.org/news/2020/05/05/jordan-free-speech-threats-under-covid-19-response

HUMAN RIGHTS WATCH (HRW). (2020b). Jordan: arrests, forced dispersal at teacher protests. Retrieved from https://www.hrw.org/news/2020/08/27/ jordan-arrests-forced-dispersal-teacher-protests

INTERNATIONAL REPUBLICAN INSTITUTE (IRI). (2018). Public opinion survey: residents of Jordan. Center for Insights in Survey Research. Retrieved from https://www.iri.org/sites/default/files/2018.11.6_jordan_poll_presentation.pdf

INTERNET CENSORSHIP MAP. (2017). Retrieved from https://www.whoishostingthis.com/blog/2017/02/27/internet-censorship/#africa

KALATHIL, S., & BOAS, T. C. (2003). Open networks, closed regimes: the impact of the Internet on authoritarian rule. Washington D.C.: Carnegie Endowment for International Peace.

KAVANAGH, J., & RICH, M. D. (2018). Truth decay: an initial exploration of the diminishing role of facts and analysis in American public life. Santa Monica: RAND Corporation.

KEREMOĞLU, E., & WEIDMANN, N. B. (2020). How dictators control the Internet: a review essay. Comparative Political Studies, 53(10-11), 1690-703.

KERR, J. (2018). Information, security, and authoritarian stability: Internet policy diffusion and coordination in the former Soviet region. International Journal of Communication, 12, 3814-34.

LANNON, E. (2019). EU cybersecurity capacity building in the Mediterranean and the Middle East. Strategic sectors security & politics. IEMed Mediterranean Yearbook. Retrieved from https://biblio.ugent.be/publication/8651360/file/8651361.pdf

LEVITSKY, S., & WAY, L. (2010). Competitive authoritarianism. Hybrid regimes after the Cold War. Cambridge: Cambridge University Press.

MEBTOUL, T. (2020, July 28). Moroccan court convicts woman who claimed COVID-19 is fake news. Morocco World News. Retrieved from https://www.moroccoworldnews.com/2020/07/312804/moroccan-court-convicts-woman-who-claimed-covid-19-is-fake-news/

MUELLER, M. (2017). Will the Internet fragment? Cambridge: Polity Press.

NEMITZ, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions Royal Society A, 376(9).

NON-ALIGNED MOVEMENT (NAM). (2020). NAM working paper for the second substantive session of the UN OEWG. Retrieved from https://front.un-arm.org/wp-content/uploads/2020/04/nam-wp-to-the-oewg-final.pdf

NYE, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44-71.

OPENNET INITIATIVE. (2009). Egypt. Retrieved from https://opennet.net/research/profiles/egypt

PLATTNER, F. M., & DIAMOND, L. (Eds). (2012). Liberation technology: social media and the struggle for democracy. Baltimore: John Hopkins University Press.

REPORTERS WITHOUT BORDERS. (2016). The new press code retains prison sentences for press offences. Retrieved from https://rsf.org/en/news/new-press-code-retains-prison-sentences-press-offences

RØD, E. G., & WEIDMANN, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. Journal of Peace Research, 5(3), 338-51.

SALEH, N. (2012). Egypt's digital activism and the dictator's dilemma: an evaluation. Telecommunications Policy, 36, 476-83.

SCHEDLER, A. (2013). The politics of uncertainty. sustaining and subverting electoral authoritarianism. Oxford: Oxford University Press.

STOLTON S., & GRÜLL, P. (2021). Lawmakers call for tougher EU disinformation laws in wake of US riots. Euractive. Retrieved from https://www.euractiv.com/section/digital/news/lawmakers-call-for-tougher-eu-disinformation-laws-in-wake-of-us-riots/

UNITED NATIONS OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF ICT IN THE CONTEXT OF INTERNATIONAL SECURITY (UN OEWG). (2020). Comments by Member States on the initial pre-draft of the OEWG report. Retrieved from https://reachingcriticalwill.org/disarmament-fora/ict/oewg/documents

UNITED NATIONS OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF ICT IN THE CONTEXT OF INTERNATIONAL SECURITY (UN OEWG). (2020). Informal multi-stakeholder cyber dialogue summary report (04-10 December 2020). Retrieved from https://eu-iss.s3.eu-central-1.amazonaws.com/horizon/assets/X5Hf8NIU/informal-ms-dialogue-series_summary-report_final.pdf

WEIDMANN, N. B., & RØD, E. G. (2019). The Internet and political protest in autocracies. Oxford: Oxford University Press.

WHEELER, D. L. (2003). Egypt: building an information society for international development. Review of African Political Economy, 30(98), 627-42.

WORLD BANK. (2020). Individuals using the Internet (% of population) – Jordan. Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=JO

XU, X. (2020). To repress or to co-opt? Authoritarian control in the age of digital surveillance. American Journal of Political Science, 65(2), 309-25.

YOM, S. L. (2009). Jordan: ten more years of autocracy. Journal of Democracy, 20(4), 151-66.

ZOLLO, F. (2019). Polarization in the online public debate. ISPI Commentary. Retrieved from https://www.ispionline.it/it/pubblicazione/polarization-online-public-debate-23150

# منع الصراعات السيبرانية وعدم الاستقرار

**باتريك باولاك**
**Patryk Pawlak**
مسؤول تنفيذي في بروكسل، معهد
الاتحاد الأوروبي للدراسات الأمنية (EUISS)[1]

1) الآراء الواردة في هذا الفصل هي آراء المؤلف، ولا تعكس بالضرورة الموقف الرسمي لمعهد الاتحاد الأوروبي للدراسات الأمنية.

## المقدمة

لقد تطورت الشراكة الأمنية بين الاتحاد الأوروبي وشركاء جنوب البحر الأبيض المتوسط عبر علاقة ثلاثية تضمنت المساعدات الإنسانية، والتعاون الإنمائي، وبناء السلام. وعلى الرغم من الالتزام الذي مضى عليه ربع قرن بتحويل حوض البحر الأبيض المتوسط إلى منطقة للحوار والتبادل والتعاون، بما يضمن السلام والاستقرار والازدهار، لا تزال المنطقة تعاني من الصراعات التي تُقوِّض الاستقرار السياسي والتنمية المستدامة في جميع أنحاء المنطقة. ويضيف تزايد اعتماد الحكومات والجهات الفاعلة من غير الدول على الأدوات الحاسوبية تعقيداً إلى هذه الصورة المعقدة أصلاً، ويزيد من كشف أسباب الضعف السياسي والاقتصادي والمجتمعي في جميع أنحاء المنطقة. وبالتالي، فإن الجهود المشتركة بين الاتحاد الأوروبي وشركائه في جنوب البحر الأبيض المتوسط تهدف إلى منع نشوب النزاعات التي يتم تمكينها أو تسهيلها عبر الإنترنت، ومعالجة الأسباب الجذرية للنزاع وحلّها، مما يوفر وسيلة قيّمة للتعاون الإقليمي. وإلى جانب الالتزام باحترام القانون الدولي والنظام القائم على القواعد، تُعتبَر هذه العناصر ركائز أساسية لإطار عمل لتعزيز سلوك الدولة المسؤول في الفضاء السيبراني.

أعرب الاتحاد الأوروبي عن التزامه بهذا الإطار في مناسبات عديدة، وهو في وضع فريد يتيح له الجمع بين الشركاء الدوليين والإقليميين، وكذلك أصحاب الشأن المعنيين، للترويج لهذا الإطار في جميع أنحاء المنطقة. ويبدو هذا الهدف مهماً بشكل خاص **نظراً للوضع الأمني الهشّ في المنطقة، ولأنّ العديد من البلدان فيها تعتمد على الأدوات الإلكترونية لبناء موقفها الأمني. وهذا يعني أيضاً أنّ استخدام الأدوات الإلكترونية الهجومية والدفاعية في العلاقات بين الدول وداخلها في الشرق الأوسط وشمال أفريقيا (MENA) هو مسألة "متى يتم استخدامها" بدلاً من السؤال حول ما "إذا كان سيتم استخدامها"**. وفي منطقة الشرق الأوسط وشمال أفريقيا، "تقف الجغرافيا السياسية في نقطة انعطاف حرجة حيث أصبح المجال السيبراني خطاً أماميّاً رئيسيّاً" (Kausch, 2017).

ومع ذلك، ظلت مشاركة الاتحاد الأوروبي مع البلدان عبر البحر الأبيض المتوسط محدودة نسبيّاً حتى الآن. ونظراً لقلقه إزاء الانتهاكات المحتملة لحقوق الإنسان من قبل الجيش أو وكالات إنفاذ القانون أو المخابرات، من ناحية، ولأنَّ نظام الضوابط والتوازنات ما زال ضعيفاً في جميع أنحاء المنطقة، من ناحية أخرى، فإنّ الاتحاد الأوروبي يتصرف بحذر عندما يتعلق الأمر بمبادرات بناء القدرات الإلكترونية في المنطقة. وغالباً ما يتم الحكم على المخاطر السياسية المتعلقة بالسمعة، والناتجة عن أي إساءة استخدام محتملة للسلطة نتيجة لدعم الاتحاد الأوروبي بأنها عالية جداً، فقد لاقت طلبات التعاون الوثيق في مجال الأمن الإلكتروني من مصر ولبنان، على سبيل المثال، آذاناً صماء في ضوء الدور المتناقض لأجهزة الاستخبارات كمزودي خدمات أمنية.

إنّ الغرض من هذا الفصل هو تحليل الأهمية المتزايدة للفضاء السيبراني كساحة للمنافسة الجيوسياسية، والتأثير المحتمل لذلك على استقرار المنطقة، والدور الذي يلعبه في تشكيل هذه البيئة. إنّ الجهود المبذولة في جميع أنحاء المنطقة، لتطوير أطر أو مؤسسات تشريعية مناسبة لتعزيز المستوى العام للمناعة السيبرانية، تسير جنبًا إلى جنب مع نشر العمليات والأدوات الإلكترونية الهجومية في النزاعات السياسية أو العسكرية الجارية. وقد أشارت التقارير العامة سابقاً إلى تورط إسرائيل وإيران وتركيا، على سبيل المثال، في استخدام العمليات السيبرانية لدعم أهدافها السياسية. وبالإضافة

إلى ذلك، فإنّ التدخل العسكري للولايات المتحدة الأمريكية والتواجد المتزايد لجهات فاعلة مثل الصين وروسيا في المنطقة يزيد من تعقيد الموقف. **وإذا حدث هناك أي شيء، فإنّ التطورات المتعلقة بالإنترنت في المنطقة توضح أنّ الفضاء السيبراني هو مجرد مجال إضافي واحد لمتابعة الأهداف السياسية والاقتصادية، ولا سيّما في سياق النزاعات الموجودة مسبقاً داخل الدول أو فيما بينها.** يستند هذا الفصل إلى تحليل المصادر الأولية، مثل أنماط التصويت في الأمم المتحدة (UN) في 18 دولة في المنطقة، والخطب والمواقف المقدمة خلال اجتماعات فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي (UN OEWG) خلال عامي 2020 و 2021. وتهدف توصيات السياسة المقدمة في النهاية إلى دعم تصميم وتنفيذ مشاركة الاتحاد الأوروبي مع المنطقة، بما في ذلك المنظمات الإقليمية.

## التوترات السيبرانية في منطقة الشرق الأوسط وشمال أفريقيا

يتّسم تاريخ منطقة الشرق الأوسط وشمال أفريقيا بعدم الاستقرار، حيث يُعَّد الفضاء السيبراني مسرحاً آخر للصراعات الموجودة سابقاً على الصعيدين المحلي والإقليمي. ومنذ أول عملية إلكترونية هجومية تمت مناقشتها علناً واستُخدمت فيها برمجيات ستَكسنت (Stuxnet) الخبيثة (التي لا تزال تثير التساؤلات حتى يومنا هذا)، أصبحت المنطقة مختبراً للاستخدامات المختلفة للأدوات الإلكترونية من قبل الحكومات والجهات الفاعلة غير الحكومية. وبمرور الوقت، **تطورت منطقة الشرق الأوسط وشمال أفريقيا لتصبح واحدة من أكثر أجزاء العالم عسكرة عبر الإنترنت، إذ تستخدم الدول "الأسلحة الإلكترونية" لحلّ توتراتها السياسية أو الاقتصادية أو العسكرية المستمرة، أو تُستخدم هذه الأسلحة من قبل الحكومات كأداة قمع تستهدف سكانها.** لقد أثّر النشاط المتزايد للدولة في الفضاء السيبراني على الطريقة التي حدّدت بها العديد من الدول التهديدات الناشئة في هذا الفضاء (كما نوقش أيضاً في الفصول السابقة من هذه الدراسة). وعلى سبيل المثال، عرّفتها إيران بأنها تهديد أو استخدام للقوة من ناحية بيئة تكنولوجيا المعلومات والاتصالات (ICT)، والتدخل وإساءة استخدام تكنولوجيا المعلومات والاتصالات، والتدابير القسرية من جانب واحد، وغيرها من التدابير في بيئة تكنولوجيا المعلومات والاتصالات، والتهديدات الناشئة عن "المحتوى"، والصورة العدائية – البناء والإسناد المُفَبرَك في بيئة تكنولوجيا المعلومات والاتصالات، وعدم التوازن بين دور ومسؤولية الدول ودور ومسؤولية القطاع الخاص، وإساءة استخدام التقنيات الناشئة، وإساءة استخدام سلسلة التوريد الخاصة بتكنولوجيا المعلومات والاتصالات.

ووفقاً لبوابة الصراع السيبراني (Cyber Conflict Portal) (EU Cyber Direct, 2020)، فإنّ **معظم العمليات الإلكترونية العسكرية في جميع أنحاء المنطقة لها علاقة ثنائية ومبنية على التوترات السياسية القائمة مسبقاً بين الدول، بما في ذلك الدول من خارج المنطقة** (مثل التوترات بين إيران والولايات المتحدة الأمريكية وحلفائها). ومع ذلك، ومع مرور الوقت، أصبحت الصورة أكثر تعقيداً مع ظهور لاعبين جُدد – حكوميين وغير حكوميين – لديهم قدرات ودوافع مختلفة. ففي عام 2017، اقترحت تقارير وسائل الإعلام اعتبار اشتراك الإمارات العربية المتحدة (UAE) في الهجمات ضدّ وكالة أنباء قطر التي تحمل علامة تجارية حكومية انتهاكاً للقانون الدولي (DeYoung, 2017)، وتمّ إدراج الهجوم في نزاع أوسع بين الإمارات – وإلى جانبها المملكة العربية السعودية والبحرين ومصر – وبين قطر، حيث اتهمت هذه الدول الدوحة بدعم الجماعات الإرهابية، والتحالف

مع إيران العدو الإقليمي. وتشير التقارير الإضافية التي صدرت في فبراير 2021 إلى أنّ المملكة العربية السعودية والإمارات العربية المتحدة قد استخدمت برامج التجسس التي أنشأتها شركة إسرائيلية لاختراق الهواتف والأجهزة لصحفيين عاملين في قناة الجزيرة (Middle East Monitor, 2021). وفي واحدة من أحدث الحلقات، أصبحت دولة الإمارات العربية المتحدة هدفاً للهجمات السيبرانية بعد أن قررت تطبيع العلاقات مع إسرائيل وكسر التضامن العربي الممتد منذ زمن.

إن أحد أكثر التحديات تعقيداً هو الروابط القائمة وآليات المراقبة والسيطرة بين الوكالات الحكومية الرسمية والجهات الفاعلة غير الحكومية التي تعمل بالنيابة عنها

**إن أحد أكثر التحديات تعقيداً هو الروابط القائمة وآليات المراقبة والسيطرة بين الوكالات الحكومية الرسمية والجهات الفاعلة غير الحكومية التي تعمل بالنيابة عنها** (Mauer, 2018). وغالباً ما يكون من الصعب تحديد مسؤولية الدولة عن أعمال هذه الجهات الفاعلة، مما يُعَقّد مهمة جعل الجناة مسؤولين عن الأنشطة الإلكترونية الخبيثة. وتُعَدّ إيران من بين الدول المشتبه في قيامها بعمليات إلكترونية في المنطقة وخارجها؛ ففي أكتوبر 2020، تم تحديد عامل التهديد الإيراني المستمر والمتقدم (APT) APT35 باعتباره مسؤولاً عن الهجمات على أكثر من 100 شخص محتمل رفيع المستوى من الحضور في مؤتمر ميونيخ للأمن وقمة الفكر العشرين (Think 20) في المملكة العربية السعودية. وفي عام 2018، كشف تقرير آخر صادر عن مؤسسة الحدود الإلكتروني (Electronic Frontier Foundation (EFF, 2018 وشركة المحمول لوك آوت (Lookout) الأمنية عن عامل جديد للتهديد المستمر والمتقدّم يُدعى دارك كاراكال (Dark Caracal)، والذي كان مسؤولاً عن حملة تجسس إلكتروني ضد أهداف في أكثر من 20 دولة. تتبع المؤلفان هذا العامل الجديد الذي بدا أنه صدر من مبنى تابع لمديرية الأمن العام اللبنانية في بيروت (Electronic Frontier Foundation, 2018). وفي هذا الصدد، يشكل دور الوكلاء الإلكترونيين في جميع أنحاء المنطقة تحدياً كبيراً للاستقرار، ويُقوِّض جهود تخفيف التصعيد ومنع نشوب النزاعات التي تقوم بها جهات فاعلة مختلفة (Kavanagh & Cornish, 2020).

كما تُعَدّ المنطقة أرضًا خصبة للعمليات التي تقوم بها جهات فاعلة غير حكومية ذات دوافع سياسية. كعصابة غزة الإلكترونية، على سبيل المثال، وهي مجموعة عربية ذات دوافع سياسية تعمل في منطقة الشرق الأوسط وشمال أفريقيا، وتستهدف بشكل رئيسي مصر والإمارات العربية المتحدة واليمن. وباهاموت (Bahamut) هي مجموعة أخرى تدير حملات تجسس إلكتروني ضد مختلف القطاعات السياسية والاقتصادية والاجتماعية في الشرق الأوسط وشمال أفريقيا. وفي عام 2000، كان يُشتبه في أنّ مجموعة باهاموت كانت وراء هجمات ضدّ دبلوماسيين سعوديين، وانفصاليين سيخ، وآخرين في منطقة الشرق الأوسط وشمال أفريقيا. وبعبارة أخرى، عندما يتعلق الأمر باستخدام الدول للأدوات الإلكترونية، كلٌّ ضدّ الآخر، فقد شهدت منطقة الشرق الأوسط وشمال أفريقيا كثافة أعلى من الأنشطة الخبيثة داخل المنطقة مقارنة بأيّ جزء آخر من العالم. ولكن، وكما يلاحظ بعض المؤلفين، يمكن أن تتطور هذه المواجهة الخليجية الداخلية في الغالب إلى مواجهة جماعية أكبر، حيث تقوم العديد من القوى الإقليمية بتوسيع علاقاتها مع الصين واليابان والهند وروسيا للتحوط من حالة عدم اليقين المتعلقة باستمرارية التزام الولايات المتحدة وأوروبا (Kausch, 2017).

وبالإضافة إلى ذلك، **تفاقمت النزاعات داخل الدول بسبب الاستخدام الواسع للمراقبة الإلكترونية، وجيوش الروبوتات من قبل الحكومات القمعية ضدّ مجتمعاتها، أو ضدّ المدافعين عن حقوق الإنسان أو في وجه المعارضين السياسيين.** شهد العقد الماضي اتجاهاً عاماً عند الدول للسيطرة على الفضاء السيبراني لسكانها استجابة للدور المتنامي

لمنصات التواصل الاجتماعي[2]، ولاستخدام المنظمات الإرهابية للإنترنت؛ (يُعتبَر الربيع العربي المثال الأكثر وضوحاً لهذا الاتجاه). وفي حين أنّ الأمرين غير مرتبطين، تعاملت الحكومات في جميع أنحاء المنطقة معهما على حدّ سواء، بوصفهما تهديداً للأمن القومي يجب مواجهته من خلال استجابة حاسمة جاءت في أشكال عديدة، كانت السيطرة على الأنشطة عبر الإنترنت واحدة منها. وانخرطت بعض الدول في التجسس الإلكتروني ضد الصحفيين أو المدافعين عن حقوق الإنسان أو النشطاء، مع طمسها الخطوط الفاصلة بين حرية التعبير السياسي أو الديني والأمن القومي والخلط بينهما، ففي المغرب، وقَع قادة احتجاجات الحراك في المغرب ضحايا لحملات الهندسة الاجتماعية التي هدفت للوصول إلى هواتفهم المحمولة (Sayadi, 2019). وغالباً ما يتم اتخاذ مثل هذه التدابير على أساس قوانين الجرائم السيبرانية التي تم تبنيها مؤخراً، والتي تمنح أجهزة الأمن القومي سلطات واسعة دون تعزيز آليات سيادة القانون والقضاء المستقل في الوقت نفسه. وعلى سبيل المثال، يُلزِم قانون الجرائم السيبرانية لعام 2018 المعتمد في مصر مزودي خدمة الإنترنت بتخزين بيانات المستخدِم لطلبها المفترض من قبل وكالات الأمن (Švedkauskas, 2019). وتُعَدّ المنطقة عميلاً مهماً للتقنيات الروسية والصينية المختصة في اعتراض الاتصالات والمراقبة، أو للشركات الخاصة النشطة مثل "إن إس أو" (NSO) أو "بلاك كيوب" (Black Cube) مع امتلاكها التراخيص الممنوحة من قِبَل بعض الدول الأعضاء في الاتحاد الأوروبي بموجب نظام التصدير ذي الاستخدام المزدوج (Goslinga & Tokmetzis, 2017). وقد تمّ توثيق "صعود الاستبداد الرقمي" في جميع أنحاء المنطقة من قبل منظمة فريدوم هاوس[3] (Freedom House).

## مفارقة التنمية والأمن

إنّ أحد الدوافع الرئيسية لانخراط الاتحاد الأوروبي في البحر الأبيض المتوسط هو الافتراض بأنه لا يمكن أن يكون هناك أمن دون تنمية، أو تنمية دون أمن. وقد اتُّخِذ هذا الشعار مبرِّراً لالتزام الاتحاد الأوروبي الاقتصادي والسياسي تجاه المنطقة. ولكنّ فهم هذا الارتباط السببي ليس موجوداً دائماً في سياسات الاتحاد الأوروبي تجاه المنطقة، عندما يتعلق الأمر بإدارة الفضاء السيبراني، ولا يبدو هذا الفهم مشتركاً بين الاتحاد الأوروبي وشركائه. وفي هذا الصدد، تعكس مفارقة التنمية والأمن الظاهرة قضايا سياسية أوسع، وتُبرِز انعدام الأمن الذي تشعر به الحكومات في جميع أنحاء المنطقة.

أولاً، يُعتقد عموماً أنّ نمو القطاع الرقمي وسدّ الفجوة الرقمية يحفزان الابتكار ويعززان النمو ويقويّان الحريات. ومن حيث المبدأ، تعترف الحكومات بفوائد تكنولوجيا المعلومات والاتصالات للتنمية الاجتماعية والاقتصادية لبلدانها. وفي محاولة لتحفيز هذا النمو، غالباً ما تشدد هذه الحكومات على أنّ "الوصول إلى المعلومات الجديدة وعلوم الاتصالات وتقنياتها يجب أن يكون متاحاً لجميع البلدان"، وتعترض على أية تدابير أحادية الجانب

2) أنظر أيضاً فصول دومينيوني وألكسندرا ماريون يمنى لبن.

3) راجع تقارير "فريدوم أون ذا نت" (Freedom on the Net) التي تُنشر بانتظام على: https://freedomhouse.org/report/freedom-net

تقيّد هذا الوصول[4]. وهذا القلق ليس مجرد سمة من سمات دول مثل إيران التي يكون وصولها إلى مثل هذه التقنيات محدوداً بالفعل بسبب العقوبات التي تفرضها الولايات المتحدة الأمريكية، ولكن هناك أيضاً دول أخرى في طريقها للتعرض لضوابط أو عقوبات محتملة على الصادرات.

ثانياً، كما في حالة إيران، تؤكد الحكومات في جميع أنحاء المنطقة أيضاً أن "البعد المتعلق بالتنمية والمخاوف المتعلقة بأمن تكنولوجيا المعلومات والاتصالات يجب معالجتها بطريقة متوازنة" (UNODA, 2019). ويرتبط هذا النهج الحذر في المقام الأول بالحاجة المتصورة إلى ممارسة درجة معينة من السيادة الرقمية التي تسمح للحكومات باتخاذ قرارات مستقلة حول السياسات العامة التي تعكس قيم وثقافات كلّ مجتمع على حدة – على الرغم من أنها قد لا تتوافق تماماً مع قيم وثقافات الآخرين. وبالنسبة لبعض البلدان، أصبحت الإشارة إلى التطوير في الوقت نفسه وسيلة للمطالبة بمزيد من الأمان. ففي أحد التقارير التي قدمتها إيران إلى فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، أشارت إلى "الحق السيادي لجميع الدول الأعضاء في الأمم المتحدة في المطالبة بحقوقها ومسؤولياتها لزيادة الفوائد والمزايا الهائلة لتكنولوجيا المعلومات والاتصالات، وتخفيف الآثار المزعزعة للاستقرار الناشئة عن استخدامها الضار" (UNODA, 2019). ومع ذلك، فإن الخلافات المستمرة حول ما يمكن أن يشكل استخداماً ضارّاً أو تأثيراً مزعزعاً – وخاصة في البلدان ذات معايير حقوق الإنسان المشكوك فيها – يؤدي إلى توترات بشأن إساءة استخدام الحكومة لأدوات تكنولوجيا المعلومات والاتصالات.

قدمت المناقشة حول التهديدات الناشئة نظرة ثاقبة لما تعتبره الدول سلوكاً مقبولاً في الفضاء السيبراني

ثالثًا، قدمت المناقشة حول التهديدات الناشئة نظرة ثاقبة لما تعتبره الدول سلوكاً مقبولاً في الفضاء السيبراني، ولمقارباتها المختلفة للروابط بين الأمن والتنمية. فقد اعتبرت مصر، على سبيل المثال، عدم استخدام تكنولوجيا المعلومات والاتصالات بشكل سلمي تهديداً خطيراً للأمن والاستقرار، وكذلك للتنمية الاقتصادية وازدهار الأمم. ويتجلى هذا الرأي بشكل خاصّ في النقاش حول حماية البنية التحتية الحيوية (CI)، مثل المياه أو الطاقة أو شبكات النقل التي يجب تفسيرها على أنها قضية تنموية أساسية نظراً لاعتماد السكان المدنيين عليها. وبالتالي، تدعو مصر إلى تعهدات ملزمة قانوناً، تحظر استخدام تكنولوجيا المعلومات والاتصالات ضد مرافق البنية التحتية الحيوية التي تقدم خدمات للجمهور، أو تدعو إلى تدابير للتصدي لتهديد تكديس نقاط ضعف الأنظمة التي يمكن استغلالها لشنّ هجمات على مثل هذه البنى التحتية[5]. ومع ذلك، فإن هذا ليس بالضرورة هو الموقف الذي طرحته إسرائيل التي طلبت في تعليقاتها الأخيرة على المسودة صفر لتقرير فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، حذف الإشارات إلى المرافق الطبية والطاقة والمياه والنقل والصرف الصحي. بالنظر إلى أنّ إسرائيل متهمة بتنفيذ أول عملية هجوم إلكتروني، ستكسنت، ضد المنشآت النووية الإيرانية (Zetter, 2014) والهجمات

4) ما لم يُذكر خلاف ذلك، تستند هذه الورقة بشكل أساسي إلى المواقف التي أعربت عنها البلدان المذكورة في مناقشات فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، والمتاحة هنا: https://www.un.org/dis weapon/open-ended-working-group/

5) هذه إشارة واضحة إلى ضعف التخزين الذي أدى إلى هجمات "واناكراي" (WannaCry) و "نوتبيتيا" (NotPetya) التي كان لها عواقب اقتصادية كبيرة في جميع أنحاء العالم، مما أدى، على سبيل المثال، إلى اعتماد عقوبات إلكترونية من قبل الاتحاد الأوروبي.

ضد أنظمة الدفاع الجوي السورية في عام 2007 (Weinberger, 2007) – وكلاهما يمكن اعتبارهما بنية تحتية حيوية. ويمكن تفسير مثل هذا الطلب على أنه محاولة لتجنب المسؤولية المحتملة. وفي الوقت نفسه، يشير طلب إنشاء علاقة سببية أقلّ وضوحاً بين تعطيل أو إتلاف أو تدمير البنية التحتية الحيوية، والبنية التحتية الحيوية للمعلومات، وبين تهديد التنمية الاقتصادية وسبل العيش، وسلامة الأفراد ورفاههم في نهاية المطاف، يشير هذا الطلب إلى أنّ هذه البنية التحتية تمثل من وجهة نظر إسرائيل هدفاً أمنيّاً مشروعاً في بعض الحالات.

وفي هذا الصدد، غالباً ما يتم استخدام العلاقة بين الأمن والتنمية من قبل الحكومات في المنطقة لتحقيق هدفين، إذ إنّ الدعوات للحدّ من انتشار الأدوات الإلكترونية الهجومية، ومنع الإفراط في عسكرة الفضاء السيبراني تهدف في الواقع إلى تقييد البلدان المتقدمة تكنولوجياً بدلاً من تعزيز أجندة إلكترونية موجهة نحو التنمية. وفي الوقت نفسه، تعمل الحُجج الداعية إلى اتّباع نهج متوازن في التوفيق بين أهداف الأمن والتنمية على تبرير سيطرة الحكومات على الفضاء السيبراني (بما في ذلك استخدام تدابير المراقبة ومراقبة المحتوى) أو تبرير الاعتراض على أي تدخل خارجي مُحتمَل في السعي لتحقيق "أهداف جيوسياسية غير مشروعة".

## سلوك الدولة المسؤول في الفضاء السيبراني ومنع الصراع

يتكون إطار السلوك المسؤول للدولة في الفضاء السيبراني من أربع ركائز رئيسية تمّ تطويرها في تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي (UN GGE)، وهذه الركائز هي: تطبيق القانون الدولي في الفضاء السيبراني، والمعايير والقواعد والمبادئ، وتدابير بناء الثقة (CBMs)، وبناء القدرات. وفي مواجهة بيئة الأمن السيبراني المتدهورة، واحتمال نشوب صراع وتصعيد في المنطقة، كما هو موضح سابقاً، فإنه من المدهش حقاً أنّ عدداً قليلاً فقط من دول الشرق الأوسط وشمال أفريقيا ساهم بفعالية في تحديد هذه السياسات وتشكيل النقاش الدولي حولها. ووسط الأصوات الصامتة إلى حدّ ما في المنطقة، نجد أنّ مصر وإيران لهما صوت مرتفع. لكنّ ما هو غير واضح هو: إلى أي مدى تعكس وجهات نظريهما إجماعاً أوسع عبر المنطقة أو هل يُقصد منها المساهمة في تشكيل مثل هذا الإجماع؟ بمعنى آخر، هل إيران ومصر تتحدثان عن المنطقة أم معها؟

وفي الوقت نفسه، وفي حين أنّ دولاً مثل تركيا أو إسرائيل، اللتين تمّ الاعتراف بقدراتهما على أنها مهمة، ولم تشاركا على نطاق واسع في العمليات الدبلوماسية الجارية، فإن أفعالهما تتحدث بصوت أعلى من أقوالهما. تشارك إسرائيل، على سبيل المثال، في تعزيز التعاون الثنائي في مجال الأمن السيبراني في المنطقة، بما في ذلك مع الدول الأعضاء في الاتحاد الأوروبي مثل قبرص أو اليونان. وفي أبريل 2021، بدا أنّ إسرائيل اعترفت بتورطها في هجوم سيبراني على منشأة إيران النووية في نطنز (أحد المكونات الرئيسية لبرنامج إيران النووي). لكنّ إسرائيل نفسها هي هدف متكرر للأنشطة السيبرانية الخبيثة أيضاً؛ ففي مايو 2021، ادّعت العديد من الشركات الإسرائيلية أنها ضحايا لهجمات إلكترونية مرتبطة بإيران. ومن ناحية أخرى، اعتمدت تركيا بشكل أكبر على مجموعات القرصنة أو الوطنيين السيبرانيين الذين استخدموا أنشطة إلكترونية خبيثة للتعبير عن استيائهم من أي آراء تنتقد سياسات أنقرة. ففي ديسمبر 2020، تعرضت المحكمة الأوروبية لحقوق الإنسان لهجوم سيبراني واسع النطاق بعد

أن نشرت حكماً ينتقد تركيا. وأعلنت مجموعة قراصنة *فريق محرابي العنقاء* (Anka Neferler Timi) مسؤوليتها عن هذا الهجوم وهجمات سابقة ضد أهداف في اليونان.

تُركّز الأقسام التالية من هذا الفصل على المواقف التي عبَّرت عنها الحكومات في العمليات الرسمية التي تقودها الأمم المتحدة.

## القوى الإقليمية: أغلبية صامتة

على الرغم من عضوية بعض الدول مثل **الأردن والجزائر والمغرب وعمان ولبنان وإسرائيل وتركيا** في فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي، والدور الذي يمكن أن تلعبه هذه الدول في تشكيل النقاش حول الاستقرار السيبراني في منطقة الشرق الأوسط وشمال أفريقيا والخليج، فإن هذه الدول كانت غائبة إلى حدّ ما. وهذا أمر مخيب للآمال – وخصوصاً في حالتي الأردن والمغرب – بصفتهما عضوين في فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي الذي قدم تقريره النهائي في يونيو 2021 (UN, 2021). وفي حالة البلدان الأخرى التي يمكن أن تلعب دوراً مهماً في التقريب بين الأطراف المختلفة. لعبت عُمان، على سبيل المثال، دوراً أساسيّاً في تطوير الاتفاق النووي الإيراني، وفي تقديم الدعم خلال الأزمة اليمنية (Winder, 2020). وقد سمحت سياسة **عُمان** البعيدة عن الأضواء نسبيّاً، وسياستها الخارجية المبنية على الحياد، بممارسة نفوذ كبير وراء الكواليس، والعمل كوسيط بين القوى الإقليمية المتنافسة مثل إيران وإسرائيل والمملكة العربية السعودية (Bodetti, 2020)، ولكنّها تظل صامتة بشأن القضايا الحاسمة في النقاش حول الاستقرار السيبراني. تقدم الأقسام التالية سرداً محدوداً لوجهات النظر والمواقف التي أعربت عنها تلك البلدان فيما يتعلق بأولوياتها.

دعا الأردن في إحدى المداخلات النادرة في فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، إلى تركيز المناقشة حول مسألتين على وجه الخصوص: وضع معايير لمواجهة التهديدات والتحديات التي تواجه المجتمع الدولي، والإشارة بوضوح إلى تلك المعايير التي تسهل التعاون الدولي، وكذلك تحديد التهديدات والتحديات المتبادلة. كما شدّد على الدور الرئيسي لوكالات الأمم المتحدة والمنظمات الإقليمية في بناء الشمول الرقمي، وتعزيز المناعة السيبرانية في جميع القطاعات: الغذاء والمياه والصحة والتعليم والتنمية الاقتصادية.

وشددت **الجزائر** على أنّ الفوائد من تكنولوجيا المعلومات والاتصالات لا يجب أن تؤخذ كأمر مُسلَّم به، وسلطت الضوء أيضاً على التهديدات الناشئة عن استخدام التقنيات الرقمية، ومن هذه التهديدات: التلاعب بالمعلومات بقصد خبيث، والهجمات السيبرانية على البنية التحتية الحيوية كالمستشفيات والشبكات الكهربائية، وعسكرة الفضاء السيبراني وتسليحه من خلال تطوير القدرات الهجومية السيبرانية، ومخاطر تحويل الفضاء السيبراني إلى مسرح للعمليات العسكرية. وفي هذا الصدد، شددت الجزائر على أهمية ضمان الاحترام الكامل لمقاصد ومبادئ ميثاق الأمم المتحدة في استخدام هذه التقنيات، وهي مبادئ المساواة في السيادة، وعدم التدخل في الشؤون الداخلية، والامتناع عن استخدام القوة في العلاقات الدولية، واحترام حقوق الإنسان، والتعايش السلمي بين الدول.

إنّ دور **إسرائيل ولبنان وتركيا** دقيق بالنظر إلى مشاركتها في تنفيذ العمليات السيبرانية، وفي وضع قواعد اللعبة بحكم الأمر الواقع على الأرض. ففي حين أنّ إسرائيل – على سبيل المثال – قد تكون مشاركاً صامتاً إلى حدّ ما في فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، فإنّ أفعالها عادة ما تتحدث بصوت عالٍ. ومن المُسلّم به عموماً أنّ إسرائيل تضع معايير لما يُعتبَر سلوكاً مقبولاً وما لا يُعتبَر مقبولاً في الفضاء السيبراني؛ فقد اشتملت عملية "السهم المميت"، وهي مناورة عسكرية واسعة النطاق أجراها الجيش الإسرائيلي في أكتوبر 2020، اشتملت على عنصر إلكترونيّ يتضمن استهداف البنية التحتية وأفراد من حزب الله (Gross, 2020). وتمّ أيضاً تحديد شركة "سيركيلز" (Circles) الإسرائيلية التابعة لمجموعة "إن إس أو غروب" (NSO Group) التي تعمل في السمسرة في مجال البرمجيات الإسرائيلية، في تقرير صادر عن "سيتيزن لاب"(Citizens Lab) يكشف موردي تقنيات المراقبة في جميع أنحاء العالم (Marczak et al., 2020). وركزت المذكرات المُقدَّمة من **تركيا** على بُعدين على وجه الخصوص: تدابير بناء الثقة، وبناء القدرات. وفيما يتعلق بالأول، شدّد الموقف التركي على أهمية إنشاء قنوات اتصال بين الدول للحالات الطارئة بهدف مواجهة التهديدات السيبرانية، وتبادل المعلومات والموارد من خلال تلك القنوات، إلّا أنّ مثل هذه الآليات غير متوفرة حاليّاً في جميع أنحاء المنطقة.

وعلى الرغم من هذه التدخلات المحدودة، هناك عدد من القواسم المشتركة في المواقف المعتمَدة عبر المنطقة، وإن لم تكن متوافقة دائماً مع الاتحاد الأوروبي (انظر الجدول 1 أدناه). فقد فضّلت معظم دول المنطقة – فيما يتعلق بسلوك الدولة المسؤول في الفضاء السيبراني – عدم الاختيار بين المواقف التي قدمتها الولايات المتحدة والدول ذات التفكير المشابه، وتلك التي قدمتها روسيا والصين وداعموهما، إذ أيدت بلدان الشرق الأوسط وشمال أفريقيا كلا القرارين اللذين يسهمان في احتكار ثنائي للمبادرات على مستوى الأمم المتحدة داخل فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي، وفريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي. وفيما يتعلق بمكافحة الجرائم السيبرانية، خرجت المنطقة عن الموقف الذي تبناه الاتحاد الأوروبي، وصوّتت لدعم القرار الذي ترعاه روسيا، والذي يدعو إلى إنشاء لجنة خاصة جديدة معنية بجرائم الإنترنت، مع وجود صكّ دولي مُلزِم كنتيجة محتملة.

**الجدول 1 :** أنماط التصويت في الجمعية العامة للأمم المتحدة على القرارات الرئيسية المتعلقة بالفضاء السيبراني:

| | الجريمة السيبرانية | الأمن الدولي وتكنولوجيا المعلومات والاتصالات | | التصرف المسؤول | |
|---|---|---|---|---|---|
| | 2019 A/RES/74/247 | 2019 A/RES/74/29 | 2020 A/RES/75/240 | 2019 A/RES/74/28 | 2020 A/RES/75/32 |
| الجزائر | نعم | نعم | نعم | نعم | نعم |
| البحرين | امتنع عن التصويت | نعم | نعم | نعم | نعم |
| مصر | نعم | نعم | نعم | لا | امتنع عن التصويت |
| إيران | نعم | نعم | نعم | لا | لا |
| إسرائيل | لا | لا | لا | نعم | نعم |
| الأردن | نعم | نعم | نعم | نعم | نعم |
| الكويت | نعم | نعم | نعم | نعم | نعم |
| لبنان | نعم | نعم | نعم | امتنع عن التصويت | امتنع عن التصويت |
| ليبيا | نعم | نعم | امتنع عن التصويت | نعم | نعم |
| المغرب | امتنع عن التصويت | نعم | نعم | نعم | نعم |
| عمان | نعم | نعم | نعم | نعم | نعم |
| قطر | نعم | نعم | نعم | نعم | نعم |
| العربية السعودية | امتنع عن التصويت | نعم | نعم | نعم | نعم |
| سوريا | نعم | نعم | نعم | لا | لا |
| تونس | امتنع عن التصويت | نعم | نعم | نعم | نعم |
| تركيا | امتنع عن التصويت | امتنع عن التصويت | لا | نعم | نعم |
| الإمارات العربية المتحدة | نعم | نعم | نعم | نعم | نعم |
| اليمن | نعم | نعم | نعم | نعم | نعم |
| الاتحاد الأوروبي | لا | امتنع عن التصويت | لا | نعم | نعم |

المصدر: تجميع المؤلف استناداً إلى بيانات من الجمعية العامة للأمم المتحدة (2019 a-c & 2020 a-b).

ملاحظة: يشير اللون الرمادي الفاتح إلى نفس التصويت من قبل الاتحاد الأوروبي ودولة ثالثة، بينما يشير اللون الرمادي الداكن إلى التصويت المعاكس، بينما يشير اللون الأبيض إلى عدم وجود تضارب في المواقف المعبر عنها.

إنّ أحد البنود التي يبدو أنّ هناك اتفاقاً شاملاً حولها عبر المنطقة هو دعم المعاهدات الدولية الجديدة. ووفقاً للجزائر، فإنّ المعاهدة الجديدة التي تأخذ في الاعتبار "اهتمامات ومصالح جميع الدول" من شأنها أن تسهم في تقييد الإجراءات التي قد تؤدي إلى زعزعة الاستقرار، ومن شأنها أن تكون أيضاً "مكرَّسة بالكامل للتعاون الدولي بهدف حماية الاستخدامات السلمية لتكنولوجيا المعلومات والاتصالات[6]". كان الوفد السوري لدى فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، أكثر صراحة في هذا الموضوع، مدعياً أنّ "بعض الدول تعتقد أنّ غياب مثل هذه الأداة يسمح للدول الأخرى بأن تتصرف بشكل غير مسؤول، وأن تُطوِّر القدرات الإلكترونية التي يمكن استخدامها ضدّ الدول الأخرى". وبالمثل، يبدو أنّ هناك تقارباً في وجهات النظر في جميع أنحاء المنطقة، عندما يتعلق الأمر بمكافحة الجرائم السيبرانية بين العديد من البلدان التي تعتبر مكافحة "الإرهاب السيبراني" و "الاستخدام الإرهابي لتكنولوجيا المعلومات والاتصالات" تهديداً خطيراً. ومع ذلك، فإنّ عدم وجود تعريف مقبول عالميّاً للإرهاب في المنطقة – أو للجريمة السيبرانية في هذا الصدد، وبسبب النطاق الواسع للتعريفات المعتمدة على المستوى الوطني، يصبح التعاون بشأن هذا الموضوع أمراً صعباً إلى حدّ ما. وقد تُرجِم ذلك أيضاً إلى آراء حول بناء القدرات في مجال الأمن السيبراني، والتي، كما عبرت عنها تركيا، "ينبغي أن تتحقق دون شروط" (UNODA, 2021b).

## مصر وإيران: تحديات منهجية

لا شك في أنّ لكلٍّ من إيران ومصر مصلحة واضحة في إسماع صوتيهما. وعلى الرغم من أنّ هدفهما النهائي المتمثل في تقليص التأثير الغربي على حوكمة الفضاء السيبراني وموارده (من حيث البنية التحتية والتنظيم و"احتكار السلطة" على سبيل المثال)، يبدو متداخلاً، فإنّ كلّاً منهما يتابع هذا الهدف بنهج مختلف. **فبينما اختارت مصر متابعة طريق الاعتراض المعتدل من خلال الاعتراف بالتقدم المُحرَز حتى الآن، والتشديد على الحاجة إلى مزيد من العمل، فقد اعترضت إيران على المؤتمر السابق واعتمدت نهجاً يدعو إلى التعديل والمراجعة على نحو أكبر.** فلا يمكن – من وجهة نظر إيران – قراءة تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي لعام 2015 الذي أقرته الجمعية العامة للأمم المتحدة، كوثيقة إجماع نظراً لأنه تمّت صياغته والاتفاق عليه من قبل عدد صغير من البلدان. ومع ذلك، يجب الاعتراف بالدرجة الكبيرة من الالتقاء في مواقفهما (انظر الجدول 2) وتلبيتها، ولا سيما بالنظر إلى تأثيرهما في تشكيل مواقف الدول الأعضاء في حركة عدم الانحياز.

لا يُعَدّ نهج إيران مفاجئاً إلى حدّ كبير، وذلك نظراً لأنه غالباً ما يتم اعتبارها "دولة مارقة" في الفضاء السيبراني بسبب عملياتها الإلكترونية الخبيثة واسعة النطاق؛ والتدخل الإيراني المزعوم في الانتخابات الرئاسية الأمريكية في عام 2020 هو مجرد مثال واحد، إذ صادرت وزارة العدل الأمريكية 92 نطاقاً مستخدماً في التضليل الإيراني العالمي، وأصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) ومكتب التحقيقات الفيدرالي

6) اقتباسات من مداخلة الجزائر في اجتماع فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، خلال الاجتماع غير الرسمي بين الدورات في سبتمبر 2019. متاحة على: https://media.un.org/en/asset/k1x/k1xubugkf4

(FBI) إنذاراً تحذيريّاً تجاه العمليات الإلكترونية التي ترعاها الدولة الإيرانية ضدّ العديد من الدول والمواقع الإلكترونية ذات الصلة بالانتخابات. وفي سبتمبر، أعلن تويتر بالفعل عن إزالة 130 حساباً إيرانيّاً ضخّمت المحادثات حول مواضيع حساسة سياسيّاً، بما في ذلك "حياة السود مهمة" (Black Lives Matter)، وقتل جورج فلويد، وقضايا أخرى تتعلق بالعدالة العرقية والاجتماعية في الولايات المتحدة. وفي النهاية، فرضت وزارة الخزانة الأمريكية عقوبات على خمسة كيانات إيرانية: الحرس الثوري الإسلامي(IRGC)، وفيلق القدس التابع للحرس الثوري الإيراني (IRGC-QF)، ومعهد بيان راسانه غوستار، وكذلك اتحاد الإذاعة والتلفزيون الإسلامي الإيراني (IRTVU) والاتحاد الدولي للوسائط الافتراضية (IUVM) المملوك أو الخاضع لسيطرة فيلق القدس.

| المسألة/الموقف | إيران | مصر |
|---|---|---|
| صك (اتفاق) دولي ملزم | نعم | نعم |
| أدوات القانون الدولي | نعم | لا |
| معايير جديدة | نعم | نعم |
| نزع العسكرة عن الفضاء السيبراني | نعم | نعم |
| حدود على تخزين نقاط ضعف الأنظمة | نعم | نعم |
| المسؤوليات المشتركة ولكن المتباينة | نعم | نعم |
| نزع الاحتكار عن الموارد | نعم | لا |
| دعم فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي | نعم | نعم |
| دعم برنامج العمل | لا | نعم |
| جدوى تدابير بناء الثقة | لا | نعم |
| درجة الطعن | مرتفعة | معتدلة |

المصدر: تجميع المؤلف استناداً إلى المواقف التي تم التعبير عنها خلال اجتماع فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي (2019–2021).

ورداً على ذلك، تنتهج إيران نهجاً متماسكاً مبنيّاً على ركيزتين: (1) تقويض مطالب الغرب بأرضية أخلاقية أعلى عندما يتعلق الأمر بالفضاء السيبراني من خلال كشف عملياتها الإلكترونية، والتشديد على المضي قدُماً في عسكرة الفضاء السيبراني الذي تضطلع فيه، و (2) اقتراح تفسيرات بديلة لمبادئ القانون الدولي الحالية وقواعد السلوك

المسؤول في الفضاء السيبراني. ويتمثل الهدف النهائي لهاتين الركيزتين في إضعاف الرواية الغربية حول تصرفات إيران الهجومية وغير المسؤولة في الفضاء السيبراني، وبالتالي تحدي مصداقية نظام العقوبات، "الإجراءات القسرية أحادية الجانب" التي تم وضعها، والتي حدّت بشكل كبير من قدرة إيران على مدى السنوات الماضية في الوصول إلى التقنيات الجديدة. ويتم ترويج هذا الرواية الإيرانية بمهارة، تحت ستار الحاجة إلى مزيد من بناء القدرات الإلكترونية من أجل دعم التقدّم التنموي وتطويره.

ومن الآليات لتحقيق ذلك دور إيران النشط في تشكيل الحوار حول تطبيق **القانون الدولي** الحالي على الفضاء السيبراني من خلال التأكيد على أنّ "قابلية تطبيق القانون الدولي الحالي في المجالات المتعلقة بالإنترنت لا يزال مجالاً غير واضح"، والتأكيد على الحاجة إلى إطار قانوني جديد متعدد الأطراف وشامل لبيئة سليمة لتكنولوجيا المعلومات والاتصالات. تقدم إيران حجة مثيرة للاهتمام مفادها أنّ القانون الدولي المتصور باعتباره "تراثاً مشتركاً للبشرية" سيشمل عدم التخصيص وإدارة مشتركة، وسيشمل أيضاً النزاهة وحق الدول الأصيل في الوصول والالتزام بنقل التكنولوجيا. وعلاوة على ذلك، لا ينبغي أن تكون مجموعة القوانين الجديدة الخاصة بالفضاء السيبراني مفتوحة "للتلاعب والتفسير المتحيز من قبل أولئك الذين يهيمنون على بيئة تكنولوجيا المعلومات والاتصالات، ولا سيما الدول ذات الاستراتيجيات والقدرات الإلكترونية الهجومية" (UNODA, 2020b).

وفيما يتعلق بقواعد ومبادئ القانون الدولي المحددة، تهدف حجج إيران – وإلى حد ما تلك التي قدمتها مصر ودول أخرى في المنطقة، كما نوقش سابقاً – إلى كبح العمليات الإلكترونية المحتمَلة من قبل الغرب ضدّ أهداف في المنطقة. ينبع هذا النهج مباشرة من الطريقة التي ترى بها المنطقة التهديدات الرئيسية في الفضاء السيبراني. وتتصدر القائمة الهجمات السيبرانية ضدّ البنية التحتية المدنية الحيوية وأنظمة المعلومات المرتبطة بها. وإدراكاً لحقيقة أنّ الخطوط الفاصلة بين البنية التحتية للمعلومات المدنية والعسكرية غالباً ما تكون غير واضحة، فإن أيّ هجوم إلكتروني قد يكون له في النهاية عواقب سلبية على السكان المدنيين. ولذلك، فإنّ "تخزين نقاط ضعف الأنظمة"، وأمن سلسلة التوريد، والمخاطر المرتبطة بالاستخدامات الضارة "لتقنيات الحوسبة الجماعية" أو "الهجمات السيبرانية المستقلة" قد وفرت سياقاً لتقديم مطالَبات ملموسة حول إيجاد قانون دولي.

لقد كانت إيران صريحة، وخصوصاً، فيما يتعلق بجميع أشكال التدخل في الشؤون الداخلية أو الخارجية للدول الأخرى، من خلال الطرق والوسائل المتعلقة بالفضاء السيبراني، بشكل مباشر أو غير مباشر، ولأي سبب من الأسباب. وشددت في تقاريرها على الحاجة إلى تعزيز دور الدول باعتبارها تتحمل المسؤولية الأساسية في الحفاظ على "بيئة تكنولوجيا المعلومات والاتصالات آمنة ومأمونة وموثوقاً بها"، ولا سيّما من خلال تعزيز سيادة الدولة "دون التأثير على حقوق الدول في اختيار نماذج التنمية والحوكمة والتشريع [...]" (UNODA, 2020a). ويرتبط هذا بشكل مباشر بالقلق الذي تعرب عنه إيران بانتظام بشأن الإجراءات القسرية أحادية الجانب. وبناءً على ذلك، قدمت إيران معياراً جديداً حيث "يجب على الدول اتخاذ خطوات بطريقة تحقق التوازن بين أمنها وتطورها" بما في ذلك حق الدول في "سلسلة التوريد التي تتضمن البحث والتطوير المتعلقين بتكنولوجيا المعلومات والاتصالات، وكذلك تصنيع واستخدام ونقل منتجات وخدمات تكنولوجيا المعلومات والاتصالات" (UNODA, 2019). وعلاوة على ذلك، شدّدت إيران أيضاً على ضرورة وفاء الدول بالتزاماتها فيما يتعلق بالأفعال غير المشروعة دوليّاً، على الرغم من

لقد كانت إيران صريحة، وخصوصاً، فيما يتعلق بجميع أشكال التدخل في الشؤون الداخلية أو الخارجية للدول الأخرى، من خلال الطرق والوسائل المتعلقة بالفضاء السيبراني، بشكل مباشر أو غير مباشر، ولأي سبب من الأسباب

أنها أضافت أنّ مثل هذه الأعمال يجب أن تُنسَب إلى صاحبها بما لا يدع مجالاً للشكّ، فالإشارة إلى أنّ نشاطاً لتكنولوجيا المعلومات والاتصالات قد انطلق أو نشأ بطريقة أخرى من الإقليم أو عناصر البنية التحتية لتكنولوجيا المعلومات والاتصالات للدولة قد تكون غير كافية في حدّ ذاتها لإسناد هذا النشاط إلى تلك الدولة. وصفت إيران "بناء الصورة العدائية والمُفبرَكة" بأنه أحد التهديدات الناشئة في الفضاء السيبراني (UNODA, 2020a). وأعربت إيران أخيراً عن مخاوفها عندما يتعلق الأمر بالتركيز على عناصر مثل "الحقّ في الدفاع عن النفس" بموجب المادة 51 من ميثاق الأمم المتحدة، وقابلية تطبيق قواعد الاشتباك في النزاعات العسكرية في سياق تكنولوجيا المعلومات والاتصالات. ورأت أنّ مثل هذه المناقشات قد تضفي عن قصد أو بغير قصد الشرعية، أو تشجع على تحويل بيئة تكنولوجيا المعلومات والاتصالات إلى ساحة نزاع. وقد يؤدي التركيز المبالغ فيه على هذه الجوانب المحدَّدة، والخلافات القانونية المرتبطة بها، وتحديات الإسناد إلى تحويل الانتباه عن معالجة الأسئلة الصحيحة حول كيفية التعاون لمنع حدوث مثل هذه النزاعات في المقام الأول.

ومن ناحية أخرى، اضطلعت مصر بدور أكثر فاعلية فيما يتعلق **بقواعد ومبادئ سلوك الدولة المسؤول**. وكانت الحُجّة الرئيسية التي قدمتها مصر هي أنّ هناك حاجة إلى تكثيف الجهود الدولية لتطوير قواعد بشأن أمن تكنولوجيا المعلومات والاتصالات بما يتفق مع القانون الدولي، من أجل الحفاظ على بيئة تكنولوجيا المعلومات والاتصالات منفتحة وآمنة ومستقرة وسلمية على المدى الطويل. وبناءً على ذلك، أصرت مصر على أنّ فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، يجب أن يركز على "تحويل ورفع مستوى" التوصيات غير الملزمة الحالية التي تم اعتمادها بالفعل إلى التزامات عملية وملزمة بصورة أكبر. وتتناول على وجه التحديد سيناريوهات النزاع الأكثر صلة في بيئة تكنولوجيا المعلومات والاتصالات، في انتظار إبرام اتفاق مناسب متعدد الأطراف وملزم قانوناً. ووفقاً لمصر، فإن أنسب طريقة للمضي قدماً هي إبرام إعلان سياسي يعكس التزام الدول الأعضاء بالتوصيات الإحدى عشرة الواردة في تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي لعام 2015 وتسريع تنفيذها، ولا سيّما فيما يتعلق بالامتناع عن: (1) الإضرار عن قصد أو عن سابق إصرار أو إعاقة استخدام وتشغيل البنية التحتية المدنية الحيوية تحت أي ظرف من الظروف. (2) تقييد وصول الدول الأخرى إلى الإنترنت. (3) تخزين نقاط ضعف الأنظمة المتعلقة بتكنولوجيا المعلومات والاتصالات. (4) الإضرار بأنظمة المعلومات الخاصة بفرق الاستجابة للطوارئ المرخَّص لها في الدول الأخرى. وفيما يتعلق بالالتزامات الإيجابية، ركّز موقف مصر بشكل خاصّ على التزامات الدول بمعالجة نقاط الضعف المحتملة في البنية التحتية الوطنية، وأنظمة المعلومات الناتجة عن استخدام المهام الخفية الضارة، وتعريض سلامة سلسلة توريد منتجات تكنولوجيا المعلومات والاتصالات للخطر. كما دعت الدول إلى اتخاذ تدابير منسقَّة نحو التبادل الطوعي للمعلومات ذات الصلة بما في ذلك أفضل الممارسات والتهديدات المحتملة ونقاط الضعف. وكانت مساهمة إيران في النقاش حول المعايير أكثر إثارة للقلق بالنسبة للوضع الراهن المقبول عموماً كما تم التعبير عنه في تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي. ووفقاً لإيران، فإنّ من "السابق لأوانه" أن تتحدث الأمم المتحدة عن تنفيذ القواعد والمبادئ التوجيهية، على الرغم من أنّ للدول حق تنفيذ المعايير المتوخاة إذا رغبت. وبدلاً من ذلك، ينبغي على فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في

سياق الأمن الدولي، من وجهة النظر الإيرانية "تسريع عمله لوضع اللمسات الأخيرة على قائمة متوازنة وشاملة من المعايير أثناء العمل على مجموعة من المصطلحات المُتفَّق عليها" (UNODA, 2020a). ولكن، في النهاية، تتقارب إيران ومصر في وجهتي نظريهما في أنّ تنفيذ المعايير الطوعية لن يكون الحلّ السحري لتصرفات الدول في الفضاء السيبراني دون وجود صكّ ملزم قانوناً، ينظم سلوك الجهات الفاعلة الحكومية وغير الحكومية في الفضاء السيبراني.

وهناك جانب آخر وثيق الصلة بمنطقة الشرق الأوسط وشمال أفريقيا وهو تطوير وتنفيذ **تدابير بناء الثقة**. وكما هو موضَّح سابقاً، فإنّ مستويات عدم الثقة بين البلدان مرتفعة نسبيّاً، وينبغي، بالتالي، اعتبار التدابير التي تهدف إلى الحدّ من مخاطر تصعيد الصراع أولوية. ومع ذلك، فليس هذا هو الحال. ففي محاولة لتصحيح الوضع، دعت مصر في فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي – دعت – الدولَ إلى التوصل إلى تعريف مشترك متّفَق عليه لما يشكّل البنية التحتية الحيوية، بهدف الموافقة – حسب الاقتضاء – على حظر أيّ عمل يستخدم تكنولوجيا المعلومات والاتصالات الهجومية، عن قصد أو سبق إصرار، لإتلاف أو إعاقة استخدام وتشغيل البنية التحتية الحيوية. وتُعتبَر هذه الاقتراحات بالفعل تطوراً مهماً للغاية نظراً لأنّ الهجمات ضد البنية التحتية للطاقة أو المياه قد تكون الأكثر عرضة للتصعيد، إذ ترى مصر أنّ "التبادل الطوعي للمعلومات حول مختلف جوانب التهديدات، ونقاط الضعف الوطنية وعبر الوطنية، وكذلك أفضل الممارسات لأمن تكنولوجيا المعلومات والاتصالات، هي أدوات قوية ينبغي استخدامها حسب مقتضيات الأمور، وبطريقة أكثر منهجية وتنسيقاً، في سياق منتدى متخصص متعدد الأطراف وشامل" (UNODA, 2020c). ومن ناحية أخرى، قدمت إيران وجهة نظر معاكسة بحُجّة أنّ أصول تدابير بناء الثقة مرتبطة بالأسلحة والتاريخ العسكري، وبالتالي لا ينبغي تطبيقها في الفضاء السيبراني. وبدلاً من ذلك، ترى إيران أنّ تدابير بناء الثقة في الفضاء السيبراني يجب أن تكون مصممة وفقاً للسمات الفريدة للفضاء السيبراني، ومعالجة ما تعتبر أنه يشكلّ المصادر الرئيسية لعدم الثقة في بيئة تكنولوجيا المعلومات والاتصالات، مثل: الاحتكار في إدارة الإنترنت، وإخفاء الهوية، والاستراتيجيات السيبرانية الهجومية، وبناء الصورة العدائية، ورُهاب الأجانب وانعدام مسؤولية الشركات والمنصات الخاصة (UNODA, 2020a). إنّ الإشارة إلى حوكمة إنترنت أكثر عدلاً ليست مفاجئة بالنظر إلى اعتماد إيران على بنية تحتية للإنترنت تدار بشكل أساسي من قبل الشركات الغربية الخاصة.

وأخيراً، تشير مواقف مصر وإيران – فيما يتعلق **ببناء القدرات الإلكترونية** – إلى جانبين مختلفين تم تجاهلهما إلى حدّ كبير حتى الآن، ولكنهما يشكلان وجهات النظر في مجال السياسة العامة هذه؛ فقد شددت مصر في مداخلاتها على أهمية "**مبدأ المسؤوليات المشتركة ولكن المتباينة**" (CBDR) عندما يتعلق الأمر بالأمن السيبراني. وعلى الرغم من أنه راسخ في القانون البيئي الدولي، وتمّ إضفاء الطابع الرسمي عليه في القانون الدولي، خلال مؤتمر الأمم المتحدة لعام 1992 حول البيئة والتنمية في ريو دي جانيرو، لم تتم مناقشة "مبدأ المسؤوليات المشتركة لكن المتباينة" في سياق إدارة الفضاء السيبراني (Epstein, 2021). ومع ذلك، فإنّ هذا الاقتراح ليس مفاجئاً، نظراً لأنّ القاسم المشترك من خلال معظم المداخلات التي قدّمها ممثلو البلدان النامية يشير إلى اختلاف واضح في مستوى التقدم التكنولوجي واستخدامات الفضاء السيبراني. وبشكل عام، تُقِرّ الدول بأنّ لديها مسؤولية مشتركة في تطوير الفضاء السيبراني، وأنه ليس لدى جميع الدول القدرات لتقديم ما هو متوقع منها. إنّ تطبيق "مبدأ المسؤوليات المشتركة لكن المتباينة" على

تُقِرّ الدول بأنّ لديها مسؤولية مشتركة في تطوير الفضاء السيبراني، وأنه ليس لدى جميع الدول القدرات لتقديم ما هو متوقع منها

الأمن السيبراني من شأنه أن يخرج عن الفهم المشترك بوجوب وصول جميع الدول إلى مستوى مماثل من النضج السيبراني المقبول عالميّاً. وبدلاً من ذلك، يتطلب الأمر من المجتمع الدولي القبول بأنّ إمكانية تطبيق المعايير الصالحة للدول الأكثر تقدماً "قد تكون غير مناسبة، وذات تكلفة اجتماعية غير مبرَّرة للبلدان النامية[7]". وعلى هذا النحو، يدعو "مبدأ المسؤوليات المشتركة ولكن المتباينة" إلى القبول بأنّ كل دولة لديها مجموعة مختلفة من القدرات التي يمكنها المساهمة من خلالها في هذا المشروع. ويتوافق هذا أيضاً مع الحُجّة التي قدمتها مصر بأنّ "تقديم المساعدة والتعاون يجب أن يكون مدفوعاً بالطلب، ويتم بناءً على طلب الدولة المتلقِّيَة، مع مراعاة احتياجاتها وخصوصياتها".

قدمت إيران موقفاً مماثلاً. ومع ذلك، فإنّ تركيزها على **إلغاء احتكار موارد الإنترنت** من خلال بناء القدرات هي فكرة طُرِحَت أيضاً أمام جمهور مختلف وحسّاس للغاية تجاه الأفكار الجديدة مثل "الاستعمار التكنولوجي" (Arnold, 2005) أو "الاستعمار الرقمي" (Hicks, 2019). ترى إيران أنّ فوائد تكنولوجيا المعلومات والاتصالات لا يمكن أن تتحقق بالكامل "ما لم تتمّ تلبية الاحتياجات التكنولوجية، والبنية التحتية والمعلوماتية، بما في ذلك إلغاء الاحتكار، وتسهيل الوصول إلى العلوم والتقنيات الجديدة المتعلقة بتكنولوجيا المعلومات والاتصالات ونقلها". وكما في حالة تدابير بناء الثقة، يجب أن يعمل بناء القدرات الإلكترونية على نزع سلاح ما تسمّيه "العقوبات الرقمية الأحادية" التي تؤثر على الاستثمار في البنى التحتية لتكنولوجيا المعلومات والاتصالات، فضلاً عن الوصول إلى التقنيات الرقمية والموارد الرقمية (ومنها على سبيل المثال، عناوين بروتوكول الإنترنت، واسم نطاق النظام والشبكات). ونتيجة لذلك، ترى إيران أنّ أي تدابير من هذا القبيل سيكون لها تأثير سلبي شامل على النمو الاقتصادي والتنمية لجميع السكان. وفي الوقت نفسه، تشير أيضاً إلى أنّ بناء القدرات "يجب ألا يُخِلّ بالأمن القومي للدول ومصالحها، وبالأخلاق الاجتماعية، والنظام العام".

## الاستنتاجات والتوصيات

يُعَدّ تعزيز سلوك الدولة المسؤول في الفضاء السيبراني حجر الزاوية في الدبلوماسية السيبرانية للاتحاد الأوروبي، وهو متجذّر بعمق في طموح الاتحاد الأوروبي للعمل كمزوّد أمان، ولا سيّما في جواره. وقد شجع الاتحاد الأوروبي على الالتزام بالقانون الدولي، والمعايير والمبادئ، وتدابير بناء الثقة في الفضاء السيبراني، من خلال الأنشطة في الأمم المتحدة والمنظمات الإقليمية الأخرى. ومع ذلك، فإنّ المشاركة في هذه الموضوعات مع منطقة الشرق الأوسط وشمال أفريقيا غير موجودة إلى حدّ كبير. وهذا أمر مثير للدهشة لأنّ الاتحاد الأوروبي خصص موارد كبيرة لبناء القدرات المتعلقة بالإنترنت، بما في ذلك الجوار الجنوبي (SN).

وباعتبار أنّ التحول الرقمي قد أصبح الآن في قلب التعاون بين الاتحاد الأوروبي وبين **البلدان الشريكة، بات** من المهم تعزيز التقارب بين الاتحاد الأوروبي ودول منطقة الشرق **الأوسط وشمال أفريقيا، فيما يتعلق بالهدف المزدوج المتمثل في بناء دول ومجتمعات أكثر مناعة، بالإضافة إلى الحدّ من مخاطر النزاعات الناتجة من الاستخدام الضارّ المحتمل لتكنولوجيا المعلومات والاتصالات.** وهذا يتطلب اعترافاً لا لبس فيه

7) انظر، على سبيل المثال: الخطاب المُقدّم خلال مؤتمر الأمم المتحدة حول البيئة في ستوكهولم عام 1972: https://www.un.org/en/conferences/environment/stockholm1972

بأنّ التحول الرقمي ليس مجرد عملية تكنولوجية بل عملية سياسية أيضاً. وعليه، يقدم هذا الفصل أربع توصيات محدَّدة لتعاون الاتحاد الأوروبي مع المنطقة.

1. يجب على الاتحاد الأوروبي أن يهدف إلى **حوار سياسي أكثر قوة مع شركائه في المنطقة فيما يتعلق بمواقفهم بشأن القضايا الرئيسية المتعلقة بالفضاء السيبراني،** ولا سيّما تطبيق القانون الدولي الحالي في الفضاء السيبراني، وقواعد السلوك المسؤول للدولة. يوفر جدول أعمال جديد للبحر الأبيض المتوسط، تمّ تقديمه في فبراير 2021، فرصة جيدة لتضمين هذه القضايا في سياق أوسع لتعزيز المناعة والتحول الرقمي. وفي محاولة لتعزيز معاييره ومبادئه من أجل فضاء إلكتروني مجاني ومنفتح ومستقر وآمن، لا ينبغي للاتحاد الأوروبي أن يخجل من التعبير علانية عمّا ينتظره من الشركاء في المنطقة. وفي الوقت نفسه، يجب على الاتحاد الأوروبي اتّباع استراتيجية مزدوَجة في المنطقة على أساس تعميق حواره مع مصر وإيران من أجل فهم مواقف كلٍّ منهما بشكل أفضل، وتشجيع اللاعبين الآخرين في الوقت نفسه – ولا سيّما تونس والمغرب والأردن – على أن يلعبوا دوراً أكثر نشاطاً. وهذا يتطلب أيضاً إعادة التفكير في نهج الاتحاد الأوروبي حول مبادرات بناء القدرات في المنطقة، ولا سيّما من خلال تحديد أفضل لأصحاب الشأن الرئيسيين واحتياجاتهم.

2. يجب أن يهدف تعاون الاتحاد الأوروبي مع المنطقة إلى **تعزيز نهج أصحاب الشأن المتعددين عبر المنطقة استناداً إلى حقيقة أنّ مناعة الدولة لا تسير دائماً جنباً إلى جنب مع المناعة المجتمعية.** في مقابل الاتجاهات العامة للتراجع الديمقراطي وانتهاكات حقوق الإنسان، يحتاج الاتحاد الأوروبي إلى ضمان أنّ بناء القدرات السيبرانية الذي يتمّ في المنطقة يجب أن ينطلق من نهج قائم على الحقوق، ومتمحور حول الإنسان. وهذا مهمّ بشكل خاص في سياق مكافحة الجريمة السيبرانية، في حين أنّ تعزيز قدرات وكالات إنفاذ القانون والعدالة الجنائية يحتاج إلى أن يكون مرتبطاً بشكل مباشر ببناء القدرات، وتهيئة البيئة المناسبة للجهات الفاعلة غير الحكومية للعمل. قد تشمل بعض الأفكار الملموسة للتعاون العملي (التشغيلي) برامج التبادل للخبراء الإلكترونيين ومنصات التدريب، والتدريبات الدولية من أجل تعزيز مستويات التأهب للحوادث السيبرانية الوطنية وقدرات الاستجابة، فضلاً عن تبادل الممارسات الجيدة لضمان أمن التقنيات الجديدة، بما في ذلك (5G Tooolbox) واللائحة العامة لحماية البيانات (General Data Protection Regulation). ويمكن أن يساعد الحوار السياسي أيضاً في تحسين التفاهم المتبادل، فيما يتعلق بتطبيق "مبدأ المسؤوليات المشتركة ولكن المتباينة" الذي تدعو إليه دول المنطقة باعتباره ذا صلة أيضاً في سياق الفضاء السيبراني.

3. **يجب على الاتحاد الأوروبي والمنظمات الإقليمية** – ولا سيّما جامعة الدول العربية ومجلس التعاون الخليجي (GCC) – **تعزيز تعاونهم لتطوير وتنفيذ تدابير بناء الثقة الخاصة بالمنطقة.** ويمكن أن يركّز هذا الحوار على استكشاف آليات لتنفيذ مجموعة من تدابير بناء الثقة المقترَحة بالفعل في تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي لعام 2015، وتطوير منصة إقليمية مُخصَّصة لتبادل المعلومات حول نقاط الضعف، وأفضل الممارسات، وتعزيز التعاون الدولي، وبناء القدرات. وفي نهاية المطاف، يمكن أن يكون الهدف من هذا

التعاون إنشاء منطقة سيبرانية منزوعة السلاح، مع التزام الدول بالامتناع عن استخدام الأدوات الإلكترونية ضد بعضها البعض. ويمكن أن يكون الاتحاد من أجل المتوسط (UfM) مُنفِّذاً مفيداً لتطوير مثل هذا المشروع أيضاً.

# المصادر والمراجع


ARNOLD, D. (2005). Europe, technology, and colonialism in the 20th century. History and Technology, 21(1), 85106-.

BODETTI, A. (2020, January 7). Oman strives for neutrality in the Middle East. Yale Global Online. Retrieved from https://archive-yaleglobal.yale.edu/content/ oman-strives-neutrality-middle-east

DEYOUNG, K. (2017, July 21). Qatar's investigation of cyberattack stops just short of naming suspects. Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/qatars-investigation-of-cyberattack-stops-just-short-of-naming-suspects/201720/07//de721b266-d8a-11e796-ab-5f38140b38cc_story.html

ELECTRONIC FRONTIER FOUNDATION (EFF). (2018). EFF and Lookout uncover new malware espionage campaign infecting thousands around the world. Retrieved from https://www.eff.org/nl/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around

EPSTEIN, C. (2021). Common but differentiated responsibilities. Encyclopedia Britannica. Retrieved from https://www.britannica.com/topic/common-but-differentiated-responsibilities

EU CYBER DIRECT. (2020). Cyber conflict portal. Retrieved from https://eucyberdirect.eu/content_research/cyber-conflict-portal/

GOSLINGA, M., & TOKMETZIS, D. (2017, February 23). The surveillance industry still sells to repressive regimes. Here's what Europe can do about it. The Correspondent. Retrieved from https://thecorrespondent.com/6249/the-surveillance-industry-still-sells-to-repressive-regimes-heres-what-europe-can-do-about-it/679999251459591290-a5

GROSS, J. A. (2020, October 29). With massive exercise in north, IDF prepares for war on multiple fronts. Times of Israel. Retrieved from https://www.timesofisrael.com/with-massive-exercise-in-north-idf-prepares-for-war-on-multiple-fronts/

HICKS, J. (2019, September 26). "Digital colonialism": why some countries want to take control of their people's data from Big Tech. The Conversation. Retrieved from https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048

KAUSCH, K. (2017). Cheap havoc: how cyber-geopolitics will destabilize the Middle East (GMF Policy Brief, 35). German Marshall Fund of the United States.

KAVANAGH, C., & CORNISH, P. (2020). Cyber operations and inter-state competition and conflict: the persisting value of preventive diplomacy. EU Cyber Direct. Retrieved from https://eucyberdirect.eu/content_research/cyber-operations-and-inter-state-competition-and-conflict-the-persisting-value-of-preventive-diplomacy/

MARCZAK, B., SCOTT-RAILTON, J., RAO, S. P., ANSTIS, S., & DEIBERT, R. (2020). Running in circles uncovering the clients of cyberespionage firm circles. The Citizen Lab. Retrieved from https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

MAUER, T. (2018). Cyber mercenaries: the state, hackers, and power. Cambridge: Cambridge University Press.

MIDDLE EAST MONITOR. (2021). New York Times: UAE hired NSA hackers to spy on Qatar. Retrieved from https://www.middleeastmonitor.com/20210207-new-york-times-uae-hired-nsa-hackers-to-spy-on-qatar/

SAYADI, E. (2019, April 8). Morocco's Hirak movement has gone quiet, but the crackdown on independent media continues. Access Now. Retrieved from https://www.accessnow.org/moroccos-hirak-movement-has-gone-quiet-but-the-crackdown-on-independent-media-continues/

UNITED NATIONS (UN). (2021). Report of the UN OEWG (Final report - advanced copy).

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2019a). Countering the use of information and communications technologies for criminal purposes. Statement of financial implications (A/74/610), A/RES/74/247. Retrieved from https://www.un.org/en/ga/74/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2019b). Advancing responsible state behavior in cyberspace in the context of international security, A/RES/74/28. Retrieved from https://www.un.org/en/ga/74/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2019c). Developments in the field of information and telecommunications in the context of inter-

national security, A/RES/74/29. Retrieved from https://www.un.org/en/ga/74/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2020a). Developments in the field of information and telecommunications in the context of international security. Statement of financial implications (A/75/674), A/RES/75/240. Retrieved from https://www.un.org/en/ga/75/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2020b). Advancing responsible state behaviour in cyberspace in the context of international security, A/RES/75/32. Retrieved from https://www.un.org/en/ga/75/resolutions.shtml

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2019). Submission by the Islamic Republic of Iran to the UN OEWG. Retrieved from https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/iran-submission-oewg-sep-2019.pdf

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2020a). Second submission by the Islamic Republic of Iran to the UN OEWG, February 2020.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2020b) Intervention by delegation of the Islamic Republic of Iran on International Law, 1 October 2020. Retrieved from https://front.un-arm.org/wp-content/uploads/2020/10/iran-intervention-1-october-2020.pdf

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2020c). Working Paper submitted by the Delegation of Egypt to the UN OEWG. Retrieved from https://unoda-web.s3.amazonaws.com/wp-content/uploads/ 2020/01/Egypt-Working-Paper-OEWG-ICTs1.pdf

UNITED NATIONS OFFICE FOR DISARAMAMENT AFFAIRS (UNODA). (2021a). UN OEWG Final Substantive Report. A/AC.290/2021/CRP.2.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2021b). Statement by Turkey at the informal meeting of the UN OEWG. Retrieved from : https://front.un-arm.org/wp-content/uploads/2021/02/Turkey-statement_OEWG-informal-meeting_February-2021.pdf

WEINBERGER, S. (2007, April 10). How Israel spoofed Syria's air defense system. Wired. Retrieved from https://www.wired.com/2007/10/how-israel-spoo/

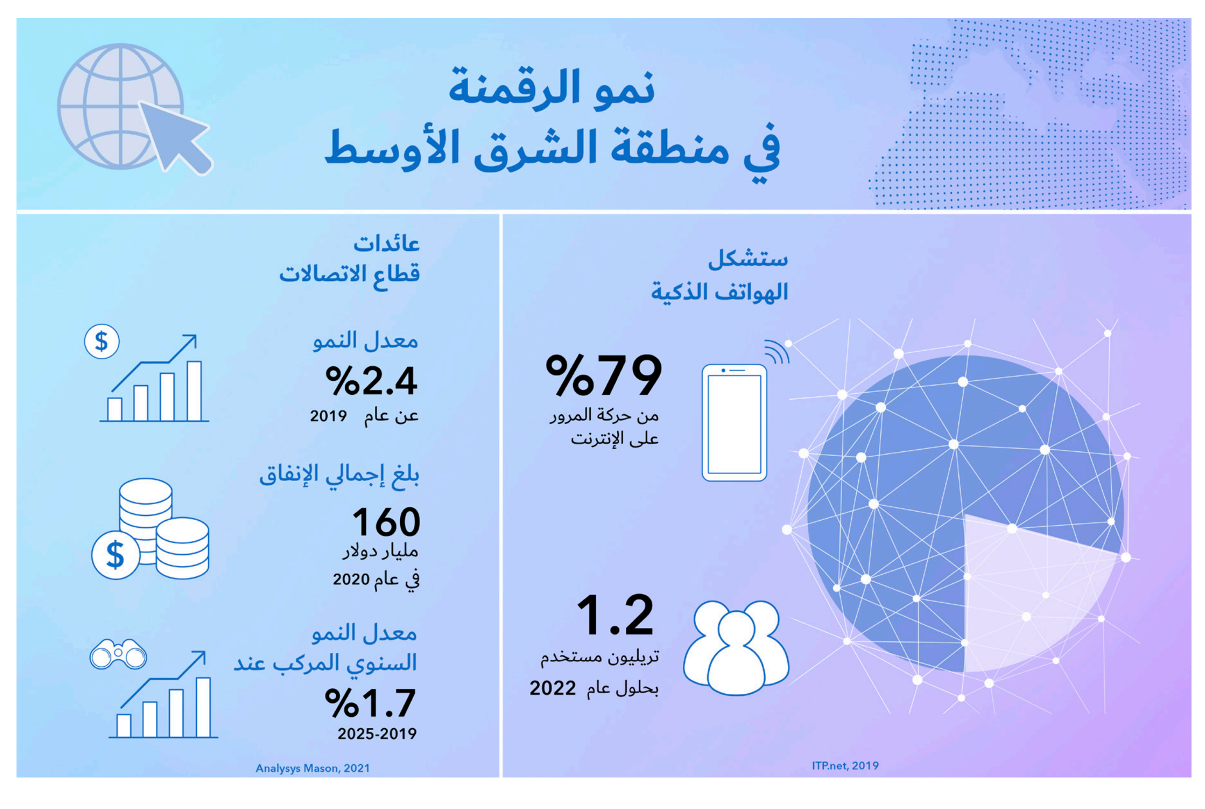
WINDER, B. (2020). Oman's regional role in a time of challenge and change. Middle East Institute. Retrieved fromhttps://www.mei.edu/publications/omans-regional-role-time-challenge-and-change

ŠVEDKAUSKAS, Ž. (2019). Three steps in ensuring digital security of Egyptian activists abroad. EuroMeSCo. Retrieved from https://www.euromesco.net/publication/three-steps-in-ensuring-digital-security-of-egyptian-activists-abroad/

ZETTER, K. (2014, March 11). An unprecedented look at Stuxnet, the world's first digital weapon. Wired. Retrieved from https://www.wired.com/2014/11/ countdown-to-zero-day-stuxnet/

# الملحق: الرقمنة والمناعة السيبرانية

**عادل عبد الصادق**
**Adel Abdel-Sadek**
خبير، وحدة الدراسات الأمنية،
مركز الأهرام للدراسات السياسية
والاستراتيجية (ACPSS)


نمو الرقمنة
في منطقة الشرق الأوسط
عائدات
قطاع الاتصالات
معدل النمو
%2.4
عن عام 2019
بلغ إجمالي الإنفاق
160
مليار دولار
في عام 2020
معدل النمو
السنوي المركب عند
%1.7
2025-2019
Analysys Mason, 2021
ستشكل
الهواتف الذكية
%79
من حركة المرور
على الإنترنت
1.2
تريليون مستخدم
بحلول عام 2022
ITP.net, 2019


أسباب تصاعد
التهديدات السيبرانية
توسيع قاعدة
المستخدمين
ضعف الوعي
بإجراءات الحماية
زيادة في
معدلات البطالة
الآثار النفسية
لتدابير العزلة الاجتماعية
زيادة في نشاط
القراصنة والمتطرفين
Abdel-Sadek, 2020
من المتوقع أن ينمو
سوق الأمن السيبراني
$28.7
مليار دولار
$16.1
مليار دولار
2020
2025
MarketsandMarkets, 2020




## المناعة السيبرانية والتنمية المستدامة في منطقة الشرق الأوسط وشمال أفريقيا (MENA)

> يتطلب اعتماد استراتيجية المناعة السيبرانية تحديد أصول البنية التحتية الحيوية (CI)، والمناطق الأكثر عرضة للتهديدات، وكذلك الجهات الفاعلة التي تقف وراءها

إنَّ "المناعة السيبرانية" تعني القدرة على الإحساس والاستعداد بشكل وقائي لمواجهة التهديدات السيبرانية ومقاومتها والاستجابة لها، سواء كانت تلك الأخطار متوقعة أم غير متوقعة، وتمكين القدرة على التعافي بسرعة من آثارها في الوقت المناسب. ويساهم التحليل الاستباقي لنقاط الضعف على جميع مستويات البيئة الرقمية الداخلية في تقليل مقدار الضرر المادي والمعنوي الذي يلحق بالمؤسسات في مختلف القطاعات (WEF, 2020) التي تشمل قطاع الطاقة، والخدمات المصرفية، والبنية التحتية للاتصالات، والرعاية الصحية، والأمن والدفاع، وسوق الأوراق المالية، والخدمات الحكومية. وتتطلب تطبيقات "المناعة السيبرانية" أن تخضع جميع الخدمات الفنية لإجراءات عديدة مثل النسخ الاحتياطي للبيانات، والتعافي من الكوارث، وإدارة الأزمات، واستمرارية الأعمال، والمناعة المؤسسية. كما يتطلب اعتماد استراتيجية المناعة السيبرانية تحديد أصول البنية التحتية الحيوية (CI)، والمناطق الأكثر عرضة للتهديدات، وكذلك الجهات الفاعلة التي تقف وراءها، سواء كانت حكومية أم غير حكومية، بما في ذلك توفّر رؤية شاملة تستند إلى مشاركة البيانات بين الحكومة والقطاع الخاص، واحتضان الاهتمام بدور الفرد والمجتمع، والتميّز في البعد الاستباقي، وتحديد ومعالجة أسباب الاضطراب والابتكار، والتطوير المستمر لمواجهة التسارع في مستوى التهديدات وطرق عملها (Carías et al., 2020).

هناك عدة أسباب وراء تحول المناعة إلى إطار عمل جذّاب للحكومات لتركيز اهتمامها عليه. أولاً، يؤدي تسريع التغيير التكنولوجي إلى تقليل القدرة على التنبؤ بالمخاطر ويتطلب ذلك مزيداً من المناعة. ثانياً، هناك وعي متزايد بالأمن السيبراني بين صانعي

القرار مع الزيادة المطّردة في التهديدات من جهة، وارتفاع تكلفتها من جهة أخرى. ثالثاً، يثير تصعيد دور الرقمنة في عمل وتكامل سلاسل التوريد العالمية، ووجود برمجيات مفتوحة المصدر أو طبيعة المكونات أو البرامج التقنية العابرة للحدود – يثير – مشاكل تتعلق بملكية الأنظمة، والولاية القضائية القانونية، ووجود أطراف ثالثة لتوفير وظائف مهمة. رابعاً، تعتمد البلدان بشكل متزايد على الخدمات الرقمية المتكاملة، مع اعتماد إنترنت الأشياء (IoT) وتطبيقات الذكاء الاصطناعي. **وأخيراً**، أصبح الاقتصاد الرقمي أكثر أهمية في تحقيق أهداف التنمية المستدامة (SDGs).

ووفقاً لمؤشر الأمن السيبراني الوطني 2020 (https://ncsi.ega.ee/ncsi-index/)، الذي يقيس استعداد الدول لمنع التهديدات السيبرانية وإدارة الحوادث السيبرانية، فإنّ الوضع في جميع أنحاء المنطقة متنوع للغاية.

## حالة وواقع المناعة السيبرانية في مصر

احتلت مصر المرتبة 23 في مؤشر الأمن السيبراني العالمي، والمرتبة 103 في مؤشر تنمية تكنولوجيا المعلومات والاتصالات، والمرتبة 84 من أصل 134 دولة في مؤشر جاهزية الشبكة (NRI) في عام 2020. وكانت مصر أيضاً من بين أفضل عشرة مُحسِّنين في الشمول الرقمي في عام 2020. وحققت المركز 81 في مؤشر الأمن السيبراني الوطني 2020 (NCSI, 2020).

### الإطار المصري للمناعة السيبرانية

**أولاً**، تتبنى مصر رؤية استراتيجية بشأن المناعة السيبرانية من خلال دستورها الذي ينصّ في المادة 31 على أنّ "أمن الفضاء السيبراني جزء لا يتجزأ من النظام الاقتصادي والأمن القومي. وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون" (Egypt Const. art. 31.). وتتطلب الأولويات الاستراتيجية لدعم القدرات الوطنية في المناعة السيبرانية قيادة فعّالة على المستويين الوطني والمحلي، وهو ما يُترجَم في بعض استراتيجيات وسياسات مصر للأمن السيبراني، مثل أهداف الاستراتيجية الوطنية للأمن السيبراني 2017–2021، ورؤية مصر 2030، واستراتيجية تكنولوجيا المعلومات والاتصالات 2030 (ICT)، وأجندة أفريقيا 2063، وأهداف التنمية المستدامة. كانت مصر تستثمر في تطوير البنية التحتية، ولم يقتصر هذا الاستثمار على تخصيص 1,6 مليار دولار في قطاع تكنولوجيا المعلومات والاتصالات فقط، بل امتدّ ليشمل قطاع الطاقة أيضاً. وحقق قطاع تكنولوجيا المعلومات والاتصالات في مصر معدل نمو قدره 15,2٪، وبلغت مساهمته في الناتج المحلي الإجمالي حوالي 4,4٪ في عام 2020 (Daily News Egypt, 2020).

**ثانياً**، أطلقت مصر في عام 2009 فريق الاستجابة للطوارئ الحاسوبية (EG-CERT)، وأنشأت في عام 2014 مجلساً أعلى للأمن السيبراني تتمثل مهمته

في زيادة الوعي، وتطوير استراتيجية للتصدي للهجمات السيبرانية من خلال الاستجابة والدعم والدفاع والتحليل. وفي عام 2019، شكلت الحكومة المصرية المجلس القومي للذكاء الاصطناعي، وعالجت شركة تريند مايكرو (Trend Micro) 14,2 مليون تهديد إلكتروني عبر البريد الإلكتروني في مصر في النصف الأول من عام 2020 (Alaa El-Din, 2020).

**ثالثاً**، في أبريل 2020، نظمت مصر عدداً من البرامج التدريبية لموظفي الحكومة على مستوى الدولة باستخدام تطبيقات التعلم السيبراني، وأطلقت العديد من المبادرات مثل تنمية المهارات الرقمية الأساسية، ووسائل التواصل الاجتماعي والسلامة على الإنترنت، وتمكين الشباب للعمل الحر، ومبادرة بناة مصر الرقمية (DEBI).

**رابعاً**، تلتزم مصر بدفع عجلة البحث والابتكار وتحديث المناهج التعليمية في المدارس والجامعات من خلال إطلاق كليات جديدة متخصصة في الذكاء الاصطناعي، واعتماد الامتحانات عبر الإنترنت، وتحسين جودة البحث العلمي داخل مراكز البحث، وتشجيع الإبداع والابتكار. أطلقت مصر مبادرات لتعزيز الابتكار مثل قادة التكنولوجيا المستقبليين (NTL)، و إنّوڤ إيجيبت (InnovEgypt)، ومركز الإبداع التكنولوجي وريادة الأعمال (TIEC)، ودورات دعم ريادة الأعمال.

**خامساً**، حققت مصر نجاحاً ملحوظاً في تنفيذ مبادرات تعزيز الشراكة مع جميع الأطراف المعنية إقليمياً ودولياً. كما يسّرت بيئة مواتية لبناء قدرات المناعة السيبرانية. ونظمت مصر التدريب وتبادل الخبرات بين فرق الاستجابة للطوارئ الحاسوبية في العالم العربي وأفريقيا (CERTs).

وأخيراً، أطلقت مصر مبادرة "مصر الرقمية" التي تشمل العمل على تطوير البنية التحتية، وتعزيز الشمول الرقمي والمالي، وتعزيز بناء القدرات والابتكار، ومكافحة الفساد، ورقمنة الخدمات الحكومية. وتم اختيار مصر لتكون العاصمة الرقمية العربية لعام 2021.

## حالة وواقع المناعة السيبرانية في تونس

احتلت تونس المرتبة 45 في مؤشر الأمن السيبراني العالمي، والمرتبة 99 في مؤشر تنمية تكنولوجيا المعلومات والاتصالات، والمرتبة 91 في مؤشر

جاهزية الشبكة، والمرتبة 96 في المؤشر الوطني للأمن السيبراني في عام 2020 (NCSI, 2020).

## الإطار التونسي للمناعة السيبرانية

**أولاً**، أطلقت تونس في عام 2019 استراتيجيتها الوطنية للأمن السيبراني، وقد اشتملت على الأهداف التالية: (1) قيادة وإدارة الفضاء السيبراني الوطني، وتعزيز العمل المشترك بين جميع الأطراف. (2) منع التهديدات الإلكترونية من خلال تعزيز القدرات الوطنية، والوعي، وحماية البنية التحتية. (3) دعم الثقة الرقمية من خلال تطوير الآليات والإجراءات. (4) تحقيق الريادة في المجال الرقمي. (5) ضمان المصالح العليا للبلاد (UNIDIR, 2019).

**ثانياً**، تعمل تونس على بناء الوعي والثقة، وحماية مواطنيها، والقطاعين العام والخاص من أي تهديد إلكتروني. وشاركت الوكالة الوطنية لأمن الحاسوب ممثلة بالفريق التونسي للاستجابة للطوارئ الحاسوبية (tunCERT) في التمرين الدولي الأول للأمن السيبراني خلال الفترة 27 أكتوبر إلى 5 نوفمبر 2020. وعلاوة على ذلك، تمّ اعتماد نظام المعلومات "ساهر" لاستدراج القراصنة ومطاردتهم، وفضح محاولات الاختراق التي تستهدف المواقع الرسمية (https://www.cert.tn/fr).

**ثالثاً**، أطلقت تونس مشروع "تواصل" لدعم شبكة مجتمعية، يقوده معهد مهندسي الكهرباء والإلكترونيات (IEEE)، ومجموعة الاهتمام الخاصة بالتكنولوجيا الإنسانية (SIGHT) (Project Tawasol, 2020). ويهدف إلى ربط المدارس الابتدائية في جميع أنحاء البلاد بالإنترنت، وتدريب الطلاب على استخدام الإنترنت من خلال ورش عمل مهارات تكنولوجيا المعلومات والاتصالات، التي ينظمها الأعضاء الشباب في معهد مهندسي الكهرباء والإلكترونيات.

**رابعاً**، تعمل تونس على تعزيز البحث والابتكار والرقمنة في التنمية الاقتصادية والاجتماعية من خلال تعزيز إنشاء مؤسسات صغيرة ومتوسطة (SMEs) جديدة ومبتكِرة، وتعزيز نمو الشركات الصغيرة والمتوسطة القائمة. كما تعمل على تطوير الشبكة الكهربائية الذكية، واستخدام الطاقة المتجددة، وتعزيز كفاءة الطاقة في النقل، وجودة شركات تكنولوجيا المعلومات والاتصالات والبنية التحتية، فضلاً عن دعم مرافق البحث والتعليم. وتشمل المؤسسات المشاركة في ذلك المدرسة الوطنية للهندسة بتونس، وجامعة تونس المنار، وجامعة منوبة، وجامعة صفاقس، والمعهد الوطني للعلوم التطبيقية والتكنولوجيا، وجامعة قرطاج (IST-Africa, 2017).

**خامسًا**، شاركت تونس في مشروع مشترك بين الاتحاد الأوروبي ومجلس أوروبا (CoE) (2017–2020) لتعزيز القدرات التشريعية والمؤسساتية بشأن الجرائم السيبرانية. وتمّ في يوليو 2017 الإعلان عن التعاون الإسباني – التونسي في مجال الأمن السيبراني. وفي أبريل 2015، أصبحت تونس عضواً في المنتدى العالمي

للخبرات الإلكترونية (UNIDIR, Tunisia 2020). لدعم السلطات التونسية بالقدرات التقنية لمواجهة التهديدات الإلكترونية. ونظّم مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) أربع دورات تدريبية حول برمجيات التحاليل الجنائية الرقمية المتخصصة، بتمويل من مكتب الولايات المتحدة للشؤون الدولية لمكافحة المخدرات وإنفاذ القانون (INL) (UNODC, 2020).

**أخيراً**، تم إطلاق "تونس الرقمية 2020" في عام 2015، بهدف خلق 80 ألف فرصة عمل في عام 2020، من خلال مزيج من استقطاب خدمات الشركات في الخارج ودول الجوار، والمشاركة في مواقع الشراكة بين القطاعين العام والخاص. وخصصت الحكومة ميزانية إجمالية تبلغ حوالي 500 مليون يورو لدعم البرنامج من خلال الحوافز والتمويل للشركات المحلية والدولية. وبالإضافة إلى ذلك، تتعاون الحكومة التونسية مع مشروع إفريقي أكبر، "أفريقيا الذكية"، وهو صندوق استثمار في الشركات الناشئة، تم إطلاقه في فبراير 2019 (Oxford Business Group, 2020).

## حالة وواقع المناعة السيبرانية في المغرب

حقق المغرب المركز 50 في مؤشر الأمن السيبراني العالمي، والمركز 100 في مؤشر تنمية تكنولوجيا المعلومات والاتصالات، والمركز 93 في مؤشر جاهزية الشبكة لعام 2020، وكذلك المركز 105 في المؤشر الوطني للأمن السيبراني (NCSI, 2020).

### الإطار المغربي للمناعة السيبرانية

**أولًا**، أقر مجلس النواب المغربي في 14 يوليو 2020 القانون 05-20 بشأن الأمن السيبراني الذي صاغته وزارة الدفاع الوطني، والذي يهدف إلى حماية البلاد والدفاع عنها من الهجمات السيبرانية بتعزيز أسس الأمن من خلال حملات التوعية والتدريب، والبحث والتطوير، وتعزيز وتطوير التعاون الوطني والدولي (Amrouche, 2021).

**ثانياً**، تصدّر المغرب الدول العشر الأولى من حيث حجم هجمات البرمجيات الخبيثة في عام 2020، إذ اكتشف كاسبرسكي (Kaspersky) ما مجموعه 13,4 مليون هجوم إلكتروني بين أبريل ويونيو 2020. وأفاد 8٪ فقط من الأشخاص الذين تم استجوابهم بأنهم يستخدمون نوعاً من برامج مكافحة الفيروسات، وأشار 18٪ إلى أنهم لا يقومون بتحديث هواتفهم المحمولة، و33٪

فقط من المستجيبين يثقون في أجهزتهم المحمولة لتخزين البيانات السرية، بينما أشار 76٪ إلى أنهم خائفون من سرقة صورهم الشخصية أو مقاطع الفيديو الخاصة بهم، وأن 39٪ ممن شملهم الاستطلاع يخشون التجسس عليهم من خلال الكاميرا (Dumpis, 2021).

**ثالثاً**، نظراً لأنّ ما يقرب من نصف السكان في المغرب هم دون سن الخامسة والعشرين، فإنّ إصلاح التعليم العالي هو أحد الاهتمامات الرئيسية لصانعي السياسات والمربين في البلاد. ولهذا السبب، بدأت وزارة التربية والتعليم مشروع رقمنة للعام الدراسي 2019–2020 مع الجامعات الحكومية في جامعة القاضي عياض بمراكش، وجامعة ابن زهر بأكادير (Mezgheldi, 2019).

**رابعاً**، قام المغرب بتكييف البحث والابتكار ليصبح قوة دافعة للتنمية الاقتصادية في سياق تنافسي بشكل خاص (Cornell University et al., 2020). ويهدف المغرب إلى أن يكون مركزاً تكنولوجيّاً بين أوروبا وأفريقيا، ورائداً في تقنيات الطاقة النظيفة، وتعزيز صناعات التكنولوجيا المستدامة.

**خامساً**، شارك المغرب أيضاً في مبادرة سايبر ساوث (CyberSouth) في 18 مايو 2017، خلال محادثات المغرب مع الناتو، وتمّ فحص آفاق التعاون في المستقبل في مجال الأمن السيبراني، ولا سيّما من خلال تبادل الخبرات والتدريب (UNIDIR, 2021).

**أخيراً**، يخطط مشروع "المغرب الرقمي" ليوجد للبلد مكاناً بين البلدان الناشئة والدول الحيوية (National Cyber Security Strategy of Morocco, 2013).

## مفتاح المناعة السيبرانية: المزيد من التعاون الإقليمي والأورومتوسطي

تم الترويج لبعض المبادرات على مدى السنوات القليلة الماضية لتعزيز التعاون الإلكتروني. ففي 20 يوليو 2020، أعلن مجلس التعاون الخليجي (GCC) عن إطلاق منصة للأمن السيبراني مختصة في تحليل البرمجيات الخبيثة كمشروع خليجي مشترك ومعتمَد من لجنة المراكز الوطنية لفرق الاستجابة للطوارئ الحاسوبية. وفي 28 يناير 2021، دعا البرلمان العربي إلى ضرورة اعتماد قواعد دولية تحكم منع نشوب حرب إلكترونية، وتعزيز التعاون الرقمي. وفي عام 2018، تمت مناقشة الاتفاقية العربية للأمن السيبراني، كما تم إحراز تقدم في مجال اعتماد قوانين لمكافحة الجريمة السيبرانية، وإنشاء مراكز وطنية للأمن السيبراني، وتعزيز التعاون الثنائي والإقليمي وفقاً لمؤشرات الأمن السيبراني العالمية.

وتمّ دمج منطقة شمال أفريقيا في الجهود الإفريقية في مجال المناعة السيبرانية، إذ تعتبر اتفاقية مالابو 2014 ركيزة مهمة لدعم الأمن السيبراني. وتمت الموافقة على استراتيجية للأمن السيبراني والجرائم السيبرانية في أفريقيا في عام 2016 من قبل وزراء الاتصالات الأفارقة. وفي عام 2018 عقد الاتحاد الإفريقي (AU) مؤتمراً سنويّاً حول الأمن السيبراني، بالتعاون مع مجلس أوروبا، مع الأخذ في الاعتبار أنّ الأمن السيبراني جزء من استراتيجية أفريقيا 2063.

تم إحراز تقدم في التعاون الثنائي والإقليمي في منطقة الشرق الأوسط وشمال أفريقيا في مجال بناء القدرات

كما تم إحراز تقدم في التعاون الثنائي والإقليمي في منطقة الشرق الأوسط وشمال أفريقيا في مجال بناء القدرات. وقد لعب المركز الإقليمي العربي للأمن السيبراني التابع للاتحاد الدولي للاتصالات (ITU-ARCC) دوراً في هذا الشأن، بالإضافة إلى مبادرات التعاون بين المنطقة والاتحاد الأوروبي مثل مبادرة سايبر ساوث أو مبادرة الاتحاد الأوروبي سايبر دايركت (Cyber Direct).

وتُعَدّ الحوسبة السحابية، ومراكز البيانات، وتطبيقات المدن الذكية فرصاً مهمة أيضاً للتعامل مع مختلف المخاطر والتحديات، مثل مشروع العاصمة الإدارية الجديدة في مصر. ويتمثل أحد أهداف رؤية المملكة العربية السعودية لعام 2030 في تحويل 10 مدن في جميع أنحاء المملكة إلى مدن ذكية. وعلاوة على ذلك، أطلقت المملكة العربية السعودية في 24 نوفمبر 2020، منظمة دولية للتعاون الرقمي (Digital Cooperation Organization, DCO)، بالتعاون مع البحرين والإمارات العربية المتحدة (UAE) والأردن والكويت وباكستان.

ومع ذلك، هناك حاجة إلى مزيد من التعاون الإقليمي لإنشاء أنظمة جديدة للكابلات البحرية ومراكز البيانات وتحديث البنية التحتية، وكذلك لزيادة قدرة اتصالات النطاق العريض، وإدارة ازدحام الشبكة، وضمان استمرارية الخدمات العامة الحيوية، وتعزيز التقنيات المالية الرقمية. وقد أظهرت أزمة كورونا أنه لا يمكن تجاوز أصحاب المصلحة المتعددين على المستويين الوطني والعالمي إلا من خلال العمل المشترك، وتبادل المعرفة، وتعبئة الموارد، وتبادل المعلومات، والتعاون والتنسيق الدوليين من أجل بناء المناعة والقدرة على الصمود في مجال الفضاء السيبراني. يجب على منطقة الشرق الأوسط وشمال أفريقيا والاتحاد الأوروبي تطوير "استراتيجية الأمن السيبراني لعموم أوروبا والبحر الأبيض المتوسط (PEMCS)"، ليس فقط للقطاع العام والبنى التحتية الحيوية، بل لمساعدة المشغلين الاقتصاديين والقطاع الخاص في مواجهة التحديات المتزايدة في التهديدات الإلكترونية أيضاً (Lannon, 2019). ويجب أن تُشكّل منطقة الاتحاد الأوروبي والشرق الأوسط وشمال أفريقيا كتلة اقتصادية رقمية، وأن تنشئ رابطة بين فِرَق الاستجابة للطوارئ الحاسوبية في كلتا المنطقتين. وأخيراً، يمكن للاتحاد الأوروبي – من خلال شراكة مع منظمة التعاون الرقمية (DCO) الجديدة – تطوير الاقتصاد الرقمي في منطقة الشرق الأوسط وشمال أفريقيا، وتحقيق أهداف التنمية المستدامة لعام 2030.

# المصادر والمراجع


ALAA EL-DIN, M. (2020). 12.4 million cyber-threats addressed in Egypt in H1 2020: trend micro. Daily News Egypt. Retrieved from https://dailynewsegypt.com/ 20204--12/30/09/million-cyber-threats-addressed-in-egypt-in-h12020--trend-micro/

AMROUCHE, A. (2021). Cybersecurity market in Morocco. Government of Canada. Retrieved from https://www.tradecommissioner.gc.ca/morocco-maroc/market-reports-etudes-de-marches/0005881.aspx?lang=eng

CARÍAS, J. F., ARRIZABALAGA, S., LABAKA, L., & HERNANTES, J. (2020). Cyber resilience progression model. Applied Sciences, 10(21), 7393. Retrieved from https://www.mdpi.com/20767393/21/10/3417-

CORNELL UNIVERSITY, INSEAD, & WIPO. (2020). The Global Innovation Index 2020: Who Will Finance Innovation? Retrieved from https://www.wipo.int/ edocs/pubdocs/en/wipo_pub_gii_2020/ma.pdf

DAILY NEWS EGYPT. (2020). Egypt's ICT sector demonstrates resilient performance despite COVID-19. Retrieved from https://dailynewsegypt.com/ 202003/12// egypts-ict-sector-demonstrates-resilient-performance-despite-covid-19/

DUMPIS, T. (2021). Kaspersky: Moroccans not concerned about cybersecurity. Morocco World News. Retrieved from https://www.moroccoworldnews.com/ 2021333890/02//kaspersky-moroccans-not-concerned-about-cybersecurity/

IST-AFRICA. (2017). National ICT research capacity and priorities for cooperation – Tunisia. Retrieved from http://www.ist-africa.org/home/default.asp? page=doc-by-id&docid=7004

KINGDOM OF MOROCCO MINISTRY OF INDUSTRY, TRADE AND NEW TECHNOLOGIES. (2013). Digital Morocco 2013: the national strategy for information society and digital economy. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Morocco_2013_Maroc_CyberSecurity_2013_ENG.pdf

LANNON, E. (2019). EU cybersecurity capacity building in the Mediterranean and the Middle East. Strategic sectors security & politics. IEMed Mediterranean Yearbook 2019. Retrieved from https://www.iemed.org/publication/eu-cybersecurity-capacity-building-in-the-mediterranean-and-the-middle-east/?lang=fr

MEZGHELDI, S. (2019). Morocco is looking for international partners in vocational training and higher education. Team Finland. Retrieved from https://www.marketopportunities.fi/home/2019/morocco-is-looking-for-international-partners-in-vocational-training-and-higher-education?type=business-opportunity&industry=education-and-learning

OXFORD BUSINESS GROUP. (2020). The report: Tunisia 2019. Retrieved from https://oxfordbusinessgroup.com/analysis/successful-start-government-working-develop-local-start-ecosystem-through-new-policies-and

PROJECT TAWASOL. (2020). Connecting primary schools to create an internet empowered next generation in Tunisia. 1 World Connected. Retrieved from https://1worldconnected.org/project/africa_digitalskills_youth_projectawasoltunisia/

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDR). (2020). Cyber security portal – Tunisia. Retrieved from file:///C:/Users/pract_doc/ Downloads/Tunisia%20(3).pdf

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). (2020). Tunisia: mobile digital forensics as a key method to prevent cybercrime. Retrieved from https://www.unodc.org/middleeastandnorthafrica/en/web-stories/tunisia_-mobile-digital-forensics-as-a-key-method-to-prevent-cybercrime.html

WORLD ECONOMIC FORUM (WEF). (2020). Rebounding from COVID-19: MENA perspectives on resilience in manufacturing and supply systems. Retrieved from https://www.weforum.org/reports/rebounding-from-covid-19-mena-perspectives-on-resilience-in-manufacturing-and-supply-systems

# قائمة الاختصارات والمصطلحات

| | | |
|---|---|---|
| **AFRIPOL** | African Police Cooperation Organisation | منظمة الشرطة الجنائية الإفريقية (الأفريبول) |
| **CBDR** | common but differentiated responsibilities | المسؤوليات المشتركة ولكن المتباينة |
| **CBM** | Confidence-building measure | تدابير بناء الثقة |
| **CEPOL** | European Union Agency for Law Enforcement Training | وكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون |
| **CERT** | Computer Emergency Response Team | فريق الاستجابة للطوارئ الحاسوبية |
| **CI** | critical infrastructure | البنية التحتية الحيوية |
| **CoE** | Council of Europe | مجلس أوروبا |
| **CSO** | Civil Society Organization | منظمة المجتمع المدني |
| **ENP** | European Neighbourhood Policy | سياسة الجوار الأوروبية |
| **EU** | European Union | الاتحاد الأوروبي |
| **GLACY** | Global Action on Cybercrime | الإجراء العالمي بشأن الجرائم السيبرانية |
| **ICT** | information and communication technologies | تكنولوجيا المعلومات والاتصالات |
| **ISP** | Internet service provider | مزود خدمة الإنترنت |
| **LEA** | Law Enforcement Agency | وكالة إنفاذ القانون |
| **MENA** | Middle East and North Africa | الشرق الأوسط وشمال أفريقيا |
| **NAM** | Non-Aligned Movement | حركة عدم الانحياز |
| **SN** | Southern Neighbourhood | الجوار الجنوبي |
| **T-CY** | Cybercrime Convention Committee | لجنة اتفاقية الجرائم السيبرانية |
| **UAE** | United Arab Emirates | الإمارات العربية المتحدة |
| **UfM** | Union for the Mediterranean | الاتحاد من أجل المتوسط |
| **UN** | United Nations | الأمم المتحدة |

| | | |
|---|---|---|
| **UN GGE** | UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security | فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بتعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي |
| **UN OEWG** | UN Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security | فريق العمل المفتوح العضوية التابع للأمم المتحدة، والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي |
| **USA** | United States of America | الولايات المتحدة الأميركية |


euromesco
Policy Study




IEMed.
European Institute of the Mediterranean